UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS

CHLOE NOFTZ, TONYA BLACK AND KENNETH WEINSTOCK, on behalf of themselves and all others similarly situated,	)	
Plaintiff	)	**Case No.** 1:24-cv-8100
v.	)	JURY TRIAL DEMANDED
KSB HOSPITAL FOUNDATION D/B/A KSB HOSPITAL F/K/A KATHERINE SHAW BETHEA HOSPITAL,	)	
Defendant.	)	

CLASS ACTION COMPLAINT AND JURY DEMAND

Plaintiffs, Chloe Noftz, Tonya Black and Kenneth Weinstock, on behalf of themselves and all others similarly situated, (hereinafter "Plaintiffs") bring this Class Action Complaint against Defendant, KSB Hospital Foundation d/b/a KSB Hospital f/k/a Katherine Shaw Bethea Hospital (hereinafter "KSB" or "Defendant"), and allege, upon personal knowledge as to their own actions, and upon information and belief as to all other matters, as follows.

INTRODUCTION

1. Plaintiffs bring this class action to address Defendant's improper practice of disclosing the confidential Personally Identifying Information ("PII")[1] and/or Protected Health Information ("PHI")[2] (collectively referred to as "Private Information") of Plaintiffs and the

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created,

proposed Class Members to third parties, including Meta Platforms, Inc. d/b/a Meta ("Facebook" or "Meta"),[3] and potentially others ("the Disclosure") via tracking technologies used on its website.

2. The Office for Civil Rights ("OCR") at the U.S. Department of Health and Human Services ("HHS") and the Federal Trade Commission ("FTC") warn about the "serious privacy and security risks related to the use of online tracking technologies" present on websites or online platforms, such as Defendant's, that "impermissibly disclos[e] consumers' sensitive personal health information to third parties."[4] OCR and FTC agree that such tracking technologies, like those present on Defendant's website, "can track a user's online activities" and "gather identifiable information about users as they interact with a website or mobile app, often in ways which are not avoidable by and largely unknown to users."[5] OCR and FTC warn that "[i]mpermissible disclosures of an individual's personal health information to third parties may result in a wide range of harms to an individual or others. Such disclosures can reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more. In addition,

---

collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed Apr. 16, 2020). KSB is clearly a "covered entity" and some of the data compromised in the Disclosure that this action arises out of is "protected health information," subject to HIPAA.

[3] Facebook changed its name from Facebook, Inc. to Meta Platforms, Inc. in October 2021. Plaintiffs' reference to both "Facebook" and "Meta" throughout this complaint refer to the same company.

[4] FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies, FEDERAL TRADE COMMISSION (July 20, 2023) https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking?utm_source=govdelivery.

[5] *Id.*

impermissible disclosures of personal health information may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others."[6]

3. Information about a person's physical and mental health is among the most confidential and sensitive information in our society, and the mishandling of medical information can have serious consequences, including discrimination in the workplace or denial of insurance coverage. If people do not trust that their medical information will be kept private, they may be less likely to seek medical treatment, which can lead to more serious health problems down the road. In addition, protecting medical information and making sure it is kept confidential and not disclosed to anyone other than the person's medical provider is necessary to maintain public trust in the healthcare system as a whole.

4. Recognizing these facts, and in order to implement requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), HHS has established "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule") governing how health care providers must safeguard and protect Private Information. Under the HIPAA Privacy Rule, no health care provider may disclose a person's personally identifiable protected health information to a third party without express written authorization.

5. In December 2022, HHS released a bulletin on its website regarding the use of tracking technologies by entities covered by HIPAA—healthcare entities like PCH—and its business associates (the "December 2022 Bulletin").[7]

---

[6] Re: Use of Online Tracking Technologies, U.S. Dep't of Health & Human Services, (July 20, 2023) (available at https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf), **attached as Exhibit A.**

[7] *See* archived version of the December 2022 Bulletin at *HHS Office for Civil Rights Issues Bulletin on Requirements under HIPAA for Online Tracking Technologies to Protect the Privacy and Security of*

6. Therein, HHS defined tracking technologies, explaining:

> Tracking technologies are used to collect and analyze information about how users interact with regulated entities' websites or mobile applications ("apps"). For example, a regulated entity may engage a technology vendor to perform such analysis as part of the regulated entity's health care operations. The HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information (PHI). Some regulated entities may share sensitive information with online tracking technology vendors and such sharing may be unauthorized disclosures of PHI with such vendors.[8]

7. In the Bulletin, HHS was clear in unambiguous terms that, "**[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules.** For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures."[9,10]

8. On March 18, 2024, HHS updated its December 2022 bulletin, "to increase clarity for regulated entities and the public" and reiterating the above basic privacy obligations.[11,12]

9. KSB is an Illinois "not-for-profit, independent healthcare provider" that operates an acute care hospital, a regional network of primary clinics, and a multi-specialty physician

---

Health Information, HHS.gov (Dec. 1, 2022), https://web.archive.org/web/20221201192812/https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

[8] *Id*.

[9] *Id*. (bold emphasis in original)

[10] Citing *to* 45 CFR 164.508(a)(3); s*ee also* 45 CFR 164.501 (definition of "Marketing").

[11] U.S. Dept. of Health and Human Svcs. Office for Civil Rights, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022, updated Mar. 18, 2024), available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html

[12] On June 20, 2024, in *American Hospital Association, et al. v. Xavier Becerra, et al.,* Case No. 4:23-cv-01110-P (N.D. Tx., Jun. 20, 2024, Doc. 67), the U.S. District Court for the Northern District of Texas vacated HHS's March 14, 2024 Bulletin as to the "Proscribed Combination," *but* acknowledged that the Proscribed Combination could be PHI in certain circumstances.

group.[13] KSB claims that each year it "reinvests in technology, facilities, and [its] employees in order to continue to meet the changing healthcare needs of [its] hometowns."[14]

10. Despite its unique position as a massive and trusted healthcare provider, KSB knowingly configured and implemented into its website, www.ksbhospital.com, (the "Website") code-based tracking devices known as "pixels" (also referred to as "trackers" or "tracking technologies"), which collected and transmitted patients' Private Information to Facebook and other third parties, without patients' knowledge or authorization.

11. Defendant encourages patients to use its Website, along with its various web-based tools and services (collectively, the "Online Platforms"), to search for physicians, locate healthcare facilities, learn about specific health conditions and treatment options, pay bills, sign up for classes and events, and more. Plaintiffs and the Class Members visited Defendant's Online Platforms in relation to their past, present, and future health, healthcare and/or payment for health care.

12. When Plaintiffs and Class Members used Defendant's Website and Online Platforms, they thought they were communicating exclusively with their trusted healthcare provider. Unbeknownst to them, Defendant embedded pixels from Facebook, Google Analytics and Google Tag Manager (together, "Google"), Innovid, CallRail, and others into its Website and Online Platforms, surreptitiously forcing Plaintiffs and Class Members to transmit intimate details about their medical treatment to third parties without their consent.

13. A tracker (also referred to as "tracking technology") is a snippet of code embedded into a website that tracks information about its visitors and their website interactions.[15] When a person visits a website with an tracker, it tracks "events" (i.e., user interactions with the site), such

[13] https://www.ksbhospital.com/about
[14] *Id.*
[15] *See* Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/

as pages viewed, buttons clicked, and information submitted.[16] Then, the tracker transmits the event information back to the website server and to third parties, where it can be combined with other data and used for marketing.[17]

14. Among the trackers Defendant embedded into its Website is the Facebook Pixel (also referred to as the "Meta Pixel" or "Pixel"). By default, the Meta Pixel tracks information about a website user's device and the URLs and domains they visit.[18] When configured to do so, the Meta Pixel can track much more, including a visitor's search terms, button clicks, and form submissions.[19] Additionally, the Meta Pixel can link a visitor's website interactions with an individual's unique and persistent Facebook ID ("FID"), allowing a user's health information to be linked with their Facebook profile.[20]

15. Operating as designed and as implemented by Defendant, the Meta Pixel allowed Defendant to unlawfully disclose Plaintiffs and Class Members' private health information, alongside identifying details to Facebook. By installing the Meta Pixel on its Website, Defendant effectively planted a bug on Plaintiffs' and Class Members' web browsers and compelled them to disclose Private Information and confidential communications to Facebook without their authorization or knowledge.

16. Facebook encourages and recommends use of its Conversions Application

[16] *See* Conversion Tracking, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking

[17] *Id.*

[18] *See* Get Started, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/get-started

[19] *See* Conversion Tracking, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking

[20] The Meta Pixel forces the website user to share the user's FID for easy tracking via the "cookie" Facebook stores every time someone accesses their Facebook account from the same web browser. "Cookies are small files of information that a web server generates and sends to a web browser." "Cookies help inform websites about the user, enabling the websites to personalize the user experience." What are Cookies?, https://www.cloudflare.com/learning/privacy/what-are-cookies/

Programming Interface ("CAPI") alongside use of the Meta Pixel.[21]

17. Unlike the Meta Pixel, which co-opts a website user's browser and forces it to transmit information to Facebook, CAPI does not cause the user's browser to transmit information directly to Facebook. Instead, CAPI tracks the user's website interactions from the website owner's private servers, which transmits the data directly to Facebook, without involvement from the website user's browser.[22, 23]

18. Because CAPI is located on the website owner's servers and is not a bug planted onto the website user's browser, it allows website owners like Defendant to circumvent any ad blockers or other denials of consent by the website user that would prevent the Meta Pixel from sending website users' Private Information to Facebook directly. For this reason, Facebook markets CAPI as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."[24]

19. Defendant utilized data from these trackers to market its services and bolster its profits. Facebook utilizes data from the Meta Pixel and CAPI to build data profiles for the purpose of creating targeted online advertisements and enhanced marketing services, which it sells for profit.

---

[21] "CAPI works with your Meta Pixel to help improve the performance and measurement of your Facebook ad campaigns." *See* Samir El Kamouny, How to Implement Facebook Conversions API (In Shopify), FETCH & FUNNEL https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/

[22] What is the Facebook Conversion API and How to Use It, REVEALBOT BLOG, https://revealbot.com/blog/facebook-conversions-api/

[23] "Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel…. This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels." Conversions API, META FOR DEVELOPERS, https://developers.facebook.com/docs/marketing-api/conversions-api

[24] About Conversions API, META FOR DEVELOPERS, https://www.facebook.com/business/help/2041148702652965

20. The information that Defendant's Meta Pixel and CAPI sent to Facebook included Private Information that Plaintiffs and Class Members submitted to Defendant's Website contained in the terms they searched, the pages they visited, and the buttons that they clicked.

21. Such information allows third parties (e.g., Facebook) to learn that a particular individual's health conditions and seeking of medical care. Facebook, in turn, sells Plaintiffs' and Class Members' Private Information to third-party marketers, who then target Plaintiffs and Class Members with online advertisements, based on the information they communicated to Defendant via the Website. Facebook and any third-party purchasers of Plaintiffs' and Class Members' Private Information also could reasonably infer from the data that a specific patient was being treated for a specific type of medical condition, such as cancer, pregnancy, dementia, or HIV.

22. In addition to the Facebook Pixel, and likely CAPI, on information and belief, Defendant installed other tracking technologies, Google Analytics, Google Tag Manager, Innovid, and CallRail, which operate similarly to the Meta Pixel and transmitted Plaintiffs' and Class Members' Private Information to unauthorized third parties.

23. Healthcare patients simply do not anticipate that their trusted healthcare provider will send their private health information to a hidden third party—let alone Facebook, a company with a sordid history of violating consumer privacy in pursuit of ever-increasing advertising revenue.

24. Neither Plaintiffs nor any Class Member signed a written authorization permitting Defendant to send their Private Information to Facebook or any other third parties uninvolved in their treatment.

25. Despite willfully and intentionally incorporating the Meta Pixel, potentially CAPI, and other third-party trackers into its Website and servers, KSB has never disclosed to Plaintiffs

or Class Members that it shared their Information with Facebook, Google, Innovid, CallRail, and possibly others.

26. Defendant further made express and implied promises to protect Plaintiffs' and Class Members' Private Information and maintain the privacy and confidentiality of communications that patients exchanged with Defendant.

27. Defendant owed common law, statutory, and regulatory duties to keep Plaintiffs' and Class Members' communications and Private Information safe, secure, and confidential.

28. Upon information and belief, KSB utilized the Meta Pixel and other tracker data to improve and to save costs on its marketing campaigns, improve its data analytics, attract new patients, and generate sales.

29. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties to those individuals to protect and to safeguard their information from unauthorized disclosure.

30. Defendant breached its statutory and common law obligations to Plaintiffs and Class Members by, *inter alia*: (i) failing to adequately review its marketing programs and web-based technology to ensure its Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share patient information; (iii) aiding, agreeing, and conspiring with third parties to intercept communications sent and received by Plaintiffs and Class Members; (iv) failing to obtain the written consent of Plaintiffs and Class Members to disclose their Private Information to Facebook and others; (v) failing to protect Private Information and take steps to block the transmission of Plaintiffs' and Class Members' Private Information through the use of Meta Pixel and other tracking technology; (vi) failing to warn Plaintiffs and Class Members; and (vii) otherwise failing to design and monitor its Website to maintain the

confidentiality and integrity of patient Private Information.

31. Plaintiffs seek to remedy these harms and bring causes of action for (I) Negligence; (II) Negligence *Per Se*; (III) Breach of Express Contract; (IV) Breach of Implied Contract; (V) Unjust Enrichment; (VI) Bailment; (VII) Violation of the Illinois Eavesdropping Statute, 720 Ill. Comp. Stat. 5/14, *et seq*.; (VIII) Violation of the Electronic Communications Privacy Act, 18 U.S.C. §§ 2511(1), *et seq.;* (IX) Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2511(3)(a) ("Unauthorized Divulgence By Electronic Communications Service"); (X) Violation of Title II of the Electronic Communications Privacy Act*,* 18 U.S.C. § 2702, *et seq*.; and (XI) Violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, *et seq.*

PARTIES

32. Plaintiff, Chloe Noftz, is a natural person and a resident and citizen of Illinois, where she intends to remain, with a principal residence in Dixon, Lee County. She is a patient of KSB and a victim of Defendant's unauthorized Disclosure of Private Information.

33. Plaintiff, Tonya Black, is a natural person and a resident and citizen of Illinois, where she intends to remain, with a principal residence in Dixon, Lee County. She is a patient of KSB and a victim of Defendant's unauthorized Disclosure of Private Information.

34. Plaintiff, Kenneth Weinstock, is a natural person and a resident and citizen of Illinois, where he intends to remain, with a principal residence in Dixon, Lee County. He is a patient of KSB and a victim of Defendant's unauthorized Disclosure of Private Information.

35. Defendant, KSB Hospital Foundation d/b/a KSB Hospital f/k/a Katherine Shaw Bethea Hospital ("KSB" or "Defendant"), is a non-profit independent healthcare corporation organized and existing under the laws of the State of Illinois with its principal place of business at 403 E. First Street, Dixon, Illinois 61021 in Lee County.

JURISDICTION AND VENUE

36. This Court has subject matter jurisdiction over the subject matter over this action under 28 U.S.C. § 1331 because it arises under the laws of the United States and under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class and at least one member o the class is a citizen of a state different from Defendant.

37. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and a substantial portion of the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

38. Venue is proper in this judicial district under 28 U.S.C. § 1391 (a) through (d) because: (i) a substantial part of the events giving rise to this action occurred in this judicial district including decisions made by Defendant's governance and management personnel or inaction by those individuals that led to the Disclosure of Plaintiffs' and Class members' Private Information; (ii) Defendant's principal place of business is located in this judicial district; (iii) Defendant collects and redistributes Class members' Private Information in this judicial district and (iv) Defendant caused harm to Class members residing in this judicial district.

COMMON FACTUAL ALLEGATIONS

A. Background

39. KSB, headquartered in Dixon, Illinois, is a healthcare provider that offers a full range of medical services including hospital medicine, birth place, medical imaging, intensive care unit, wound care, cardiology, surgery, laboratory and home health care.[25]

40. KSB operates "KSB Hospital" a "not-for-profit, independent healthcare

[25] https://www.ksbhospital.com/locations/ksbhospital

provider…[which has] grown and evolved into today's acute care hospital, [a] regional network of primary care clinics, and a multi-specialty physician group. Each year [KSB] reinvest[s] in technology, facilities, and [its] employees in order to continue to meet the changing healthcare needs of [KSB's] hometowns."[26]

41. KSB serves many of its patients via its Website and Online Platforms, which it encourages patients to use to find healthcare services and providers, access information about specific health conditions, request appointments, and more.[27] It promotes the comprehensive functionality of these tools and promotes their use, in service of its own goal of increasing profitability.

42. Defendant promotes the comprehensive functionality of these tools and promotes their use, in service of its own goal of increasing profitability. In furtherance of that goal, Defendant purposely installed the Meta Pixel and other trackers onto its Website, for the purpose of gathering information about Plaintiffs and Class Members to further its marketing efforts and profits. But Defendant did not only generate information for its own use: it also shared patient information, including Private Information belonging to Plaintiffs and Class Members, with Facebook, and other unauthorized third parties.

43. To better understand Defendant's unlawful data-sharing practices, a brief discussion of basic web design and tracking tools follows.

i. Facebook's Business Tools and the Meta Pixel

44. Facebook operates the world's largest social media company and generated $117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.[28]

[26] https://www.ksbhospital.com/about

[28] Meta Reports Fourth Quarter and Full Year 2021 Results, FACEBOOK https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx

45. In conjunction with its advertising business, Facebook encourages and promotes its "Business Tools" to be used to gather customer data, identify customers and potential customers, target advertisements to those individuals, and market products and services.

46. Facebook's Business Tools, including the Meta Pixel and Conversions API, are bits of code that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of user activity on those platforms.

47. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, clicks a button, fills out a form, and more.[29] Businesses that want to target customers and advertise their services can also create their own tracking parameters by building a "custom event."[30]

48. The Meta Pixel is a Business Tool used to "track[] the people and type of actions they take" on an website.[31] When an individual accesses a webpage containing the Meta Pixel, the communications with that webpage are instantaneously and surreptitiously duplicated and sent to Facebook, traveling directly from the user's browser to Facebook's server, based off instructions from the Meta Pixel.

49. Notably, this transmission only occurs on webpages that contain the Pixel. A website owner can configure its website to use the Pixel on certain webpages that don't implicate patient privacy, such as a homepage, and disable it on pages that do implicate patient privacy, such as Defendant's "Find a Provider" page.

---

[29]Specifications for Facebook Pixel Standard Events, META, https://www.facebook.com/business/help/402791146561655 (last visited Jan. 31, 2023); *see also* Facebook Pixel, Accurate Event Tracking, Advanced, META FOR DEVELOPERS; https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* Best Practices for Facebook Pixel Setup, META https://www.facebook.com/business/help/218844828315224; App Events API, META FOR DEVELOPERS, https://developers.facebook.com/docs/marketing-api/app-event-api/

[30] About Standard and Custom Website Events, META, https://www.facebook.com/business/help/964258670337005; *see also* Facebook, App Events API, *supra*.

[31] Retargeting, META, https://www.facebook.com/business/goals/retargeting.

50. The Meta Pixel's primary purpose is to enhance online marketing, improve online ad targeting, and generate sales.[32].

51. Facebook's own website informs companies that "[t]he Meta Pixel is a piece of code that you put on your website that allows you to measure the effectiveness of your advertising by understanding the actions people take on your website."[33]

52. According to Facebook, the Meta Pixel can collect the following data.

> **Http Headers** – Anything present in HTTP headers. HTTP Headers are a standard web protocol sent between any browser request and any server on the internet. HTTP Headers include IP addresses, information about the web browser, page location, document, referrer and ***person using the website.*** [Emphasis added.]
>
> **Pixel-specific Data** – Includes Pixel ID and the Facebook Cookie.
>
> **Button Click Data** – Includes any buttons clicked by site visitors, the labels those buttons and any pages visited as a result of the button clicks.
>
> **Optional Values** – Developers and marketers can optionally choose to send additional information about the visit through Custom Data events. Example custom data events are conversion value, page type and more.
>
> **Form Field Names** – Includes website field names like email, address, quantity, etc., for when you purchase a product or service. We don't capture field values unless you include them as part of Advanced Matching or optional values.[34]

53. Facebook boasts to its prospective users that the Meta Pixel can be used to:

- **Make sure your ads are shown to the right people.** Find new customers, or people who have visited a specific page or taken a desired action on your website.
- **Drive more sales**. Set up automatic bidding to reach people who are more likely to take an action you care about, like making a purchase.
- **Measure the results of your ads.** Better understand the impact of your ads by measuring what happens when people see them.[35]

---

[32] *See* Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/
[33] About Meta Pixel, META, https://www.facebook.com/business/help/742478679120153
[34] Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/
[35] About Meta Pixel, META, https://www.facebook.com/business/help/742478679120153

54. Facebook likewise benefits from Meta Pixel data and uses it to enhance its own ad targeting abilities.

ii. Defendant's method of transmitting Plaintiffs' and Class Members' Private Information via the Meta Pixel and/or Conversions API i.e., the Interplay between HTTP Requests and Responses, Source Code, and the Meta Pixel

55. Web browsers are software applications that allow consumers to navigate the internet and view and exchange electronic information and communications. Each "client device" (such as computer, tablet, or smart phone) accesses web content through a web browser (e.g., Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

56. Every website is hosted by a computer "server" that holds the website's contents and through which the website owner exchanges files or communications with Internet users' client devices via their web browsers.

57. Web communications consist of HTTP Requests and HTTP Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies.[36]

58. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), they also send the host server data, which is embedded inside the URL and can include cookies.

59. When an individual visits a website, their web browser sends an HTTP Request to the entity's servers that essentially asks the website to retrieve certain information. The entity's servers send the HTTP Response, which contains the requested information in the form of

[36]"Cookies are small files of information that a web server generates and sends to a web browser . . . . Cookies help inform websites about the user, enabling the websites to personalize the user experience." https://www.cloudflare.com/learning/privacy/what-are-cookies/

"Markup." This is the foundation for the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate a website.

60. Every website is comprised of Markup and "Source Code." Source Code is simply a set of instructions that commands the website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code.

61. Source code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user.

62. In this way, the Meta Pixel acts much like a traditional wiretap: intercepting and transmitting communications intended only for the website host and diverting them to Facebook.

63. Separate from the Meta Pixel, third parties place cookies in the browsers of web users. These cookies can uniquely identify the user, allowing the third party to track the user as the browse the internet—on the third-party site and beyond. Facebook uses its own cookie to identify users of a Meta-Pixel-enabled website and connect their activities on that site to their individual identity. As a result, when a Facebook account holder uses a website with the Meta Pixel, the account holder's unique Facebook ID is sent to Facebook, along with the intercepted communication, allowing Facebook to identify the user associated with the information it has intercepted.

64. With substantial work and technical know-how, internet users can sometimes circumvent these browser-based wiretap technologies. To counteract this, third parties bent on gathering data implement workarounds that are difficult for web users to detect or evade. Facebook's workaround is Conversions API, which "is designed to create a direct connection

between [web hosts'] marketing data and [Facebook]."[37] This makes Conversions API a particularly effective tool because it allows sends Facebook data directly from the website server to Facebook, without relying on the user's web browser. Notably, client devices do not have access to host servers containing Conversions API, and thus, they cannot prevent (or even detect) this transmission of information to Facebook.

65. While there is no way to confirm with certainty that a website owner is using Conversions API without accessing the website server, Facebook instructs companies like Defendant to "[u]se the Conversions API in addition to the Meta Pixel, and share the same events using both tools," because such a "redundant event setup" allows the entity "to share website events [with Facebook] that the pixel may lose."[38] Consequently, if a website owner utilizes the Meta Pixel on its website, it is also reasonable to infer that it implemented the Conversions API on its website server(s), in accordance with Facebook's documentation.

66. The Meta Pixel, Conversions API, and other third-party trackers do not provide any substantive content on the host website. Rather, their only purpose is to collect information to be used for marketing and sales purposes.

67. Accordingly, without any knowledge, authorization, or action by a user, a website owner can use its website source code to commandeer its users' computing devices and web browsers, causing them to invisibly re-direct the users' communications to Facebook and others.

68. In this case, Defendant employed the Meta Pixel and potentially Conversions API to intercept, duplicate, and re-direct Plaintiffs' and Class Members' Private Information to Facebook contemporaneously, invisibly, and without the patient's knowledge.

---

[37] About Conversions API, META, https://www.facebook.com/business/help/2041148702652965
[38] *See* Best Practices for Conversions API, META, https://www.facebook.com/business/help/308855623839366

69. Consequently, when Plaintiffs and Class Members visited Defendant's Website and communicated their Private Information, it was simultaneously intercepted and transmitted to Facebook.

iii. Defendant's Other Trackers: Google Analytics with Google Tag Manager, Innovid, and CallRail

70. Defendant also employed other trackers, including Google Analytics with Google Tag Manager ("GTM"), Innovid, and CallRail, which, on information and belief likewise transmitted Plaintiffs' and the Class Members' Private Information to third parties without Plaintiffs' and Class Members' knowledge or authorization.

71. Most basically, "Google Analytics is a platform that collects data from your websites and apps to create reports that provide insights into your business."[39] Once a business implants the Google Analytics tracking measurement code on a its website, every time a user visits a webpage, the tracking code will collect information about how that user interacted with the page.[40]

72. Google Analytics allows Defendant to track and share with Google (1) who uses its website; (2) what is performed on its website; (3) when users visit its website; (4) where on the website users perform these actions; and (5) how users navigate through the website to perform these actions. Google gathers this information using trackers embedded on KSB's Website and generates corresponding reports.[41]

73. To help Google generate reports (usually in realtime), trackers embedded in a

[39] Google, *Analytics Help, Introduction to Analytics How Google Analytics works*, avail. at https://support.google.com/analytics/answer/12159447?hl=en&ref_topic=14089939&sjid=3016588406699844463-NC

[40] *Id*.

[41] *See generally*, MarketLytics, *A big list of what Google Analytics can & cannot do*, avail. at https://marketlytics.com/blog/list-of-things-google-analytics-can-and-cannot-do/

website send Google (1) information about the user's device; (2) client- and user-specific identifiers; and (3) information about what event the user performed.

74. According to Google, "Google Tag Manager is a tag management system (TMS) that allows you to quickly and easily update measurement codes and related code fragments collectively known as ***tags*** on your website or mobile app. Once the small segment of Tag Manager code has been added to your project, you can safely and easily deploy analytics and measurement tag configurations from a web-based user interface."[42]

75. As Google goes onto describe:

> When Tag Manager is installed, your website or app will be able to communicate with the Tag Manager servers. You can then use Tag Manager's web-based user interface to set up tags, establish ***triggers*** that cause your tag to fire when certain events occur, and create ***variables*** that can be used to simplify and automate your tag configurations.
>
> A collection of tags, triggers, variables, and related configurations installed on a given website or mobile app is called a ***container***. A Tag Manager container can replace all other manually-coded tags on a site or app, including tags from Google Ads, Google Analytics, Floodlight, and 3rd party tags.[43]

76. Defendant also utilizes Innovid, which was formerly TVSquared, Innovid is a tool used to track how effective video/tv advertising is. KSB was likely using Innovid to measure the effectiveness of a video advertising campaign.

77. Further, Defendant utilizes CallRail, a tool used to compare advertising campaigns' effectiveness. CallRail does this by attributing unique phone numbers to specific ad campaigns or traffic sources. CallRail determines that a user clicked on or viewed a particular ad. CallRail will dynamically change the phone numbers the user sees on the website to the ad specific phone

[42] *See Google Tag Manager Overview,* available at https://support.google.com/tagmanager/answer/6102821?hl=EN#:~:text=Google%20Tag%20Manager%20is%20a,your%20website%20or%20mobile%20app

[43] *Id*.

number. CallRail also inserts hidden data into contact forms and online chat tools. KSB was sending CallRail the referrer and current URLS, identifying information, and users' Google Analytic IDs.

78. On information and belief, through these other trackers, Google Analytics with GTM, Innovid, and CallRail, Defendant transmitted Plaintiffs' and the Class Members' Private Information to Facebook and those other third parties without Plaintiffs' and Class Members' knowledge or authorization.

iv. Defendant Violated its Own Privacy Policies

79. KSB lists "Patient's Rights and Responsibilities" ("Patient Rights") and maintains a "Notice of Privacy Practices" ("Privacy Policy") which are both posted and maintained on Defendant's Website.[44]

80. In its enumerated Patient's Rights, KSB acknowledges that "each patient has a right to: [r]eceive safe care that respects your confidentiality and your personal privacy, values, and beliefs."[45] KSB further notes patients "have the right to know about hospital policies and procedures."[46]

81. Defendant's Privacy Policy provides, "[t]his notice describes how medical information about you may be used and disclosed and how you can get access to this information."

82. KSB's Privacy Policy further states, "**In these cases we *never* share your information unless you give us written permission:** • Marketing purposes. • Sale of your

[44] *See* KSB Patient Rights and Responsibilities, available at https://www.ksbhospital.com/your-rights-and-responsibilities/, and KSB Notice of Privacy Practices, available at https://www.ksbhospital.com/wordpress2017/wp-content/uploads/2023/07/npp_booklet_hc_provider-64a2ee1500642.pdf, attached as **Exhibits B** and **C,** respectively**.**
[45] **Ex. B.**
[46] *Id*.

information • Most sharing of psychotherapy Notes."[47]

83. Therein, KSB further acknowledges, represents and promises:

> **Our Responsibilities**
>
> • We are required by law to maintain the privacy and security of your protected health information.
>
> • We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
>
> • We must follow the duties and privacy practices described in this notice and give you a copy of it.
>
> • We will not use or share your information other than as described here unless you tell us we can in writing. If you tell us we can, you can change your mind at any time. Let us know if you change your mind.[48]

84. On information and belief, KSB does not maintain any other online website user policy that otherwise governs or discloses to its patients and its website users how KSB collects and uses their personal information when visiting the Website.

85. Despite these representations in its privacy policies Defendant does, indeed transfer Private Information including PHI to third parties for marketing purposes, without written authorization, and without patients' knowledge. Using the Meta Pixel and other tracking technologies, such as Google Analytics with Google Tag Manager ("GTN"), Innovid and CallRail, Defendant used and disclosed Plaintiffs' and Class Members' Private Information and confidential communications to Facebook, and other unauthorized third parties, without written authorization, win violation of KSB's privacy policies.

v. Defendant Unauthorizedly Disclosed Plaintiffs' and the Class's Private Information via the Meta Pixel and Related Tracking Technologies

[47] **Exhibit C** (emphasis in original).
[48] *Id*.

86. Defendant disclosed Plaintiffs' and Class Members' Private Information and confidential communications to Facebook and other third parties including Google, CallRail, and Innovid via the Meta Pixel and other tracking technologies, without Plaintiffs' and Class Members' authorization, for marketing purposes.

87. On information and belief, the information that Defendant's Meta Pixel, and possibly CAPI, sent to Facebook included the Private Information that Plaintiffs and the Class Members submitted to Defendant's Website and Online Platforms, including, *inter alia*: (i) patients' search activities; (ii) content that patients browsed; (iii) financial related activities; and (iv) patient portal and medical record related activities.

88. KSB did this through PageView, Microdata, and SubscribedButtonClick events. In each of the transmitted Meta Pixel events, KSB included the "c_user" cookie, which Facebook uses to identify users.

KSB Disclosed Patients' Search Activities

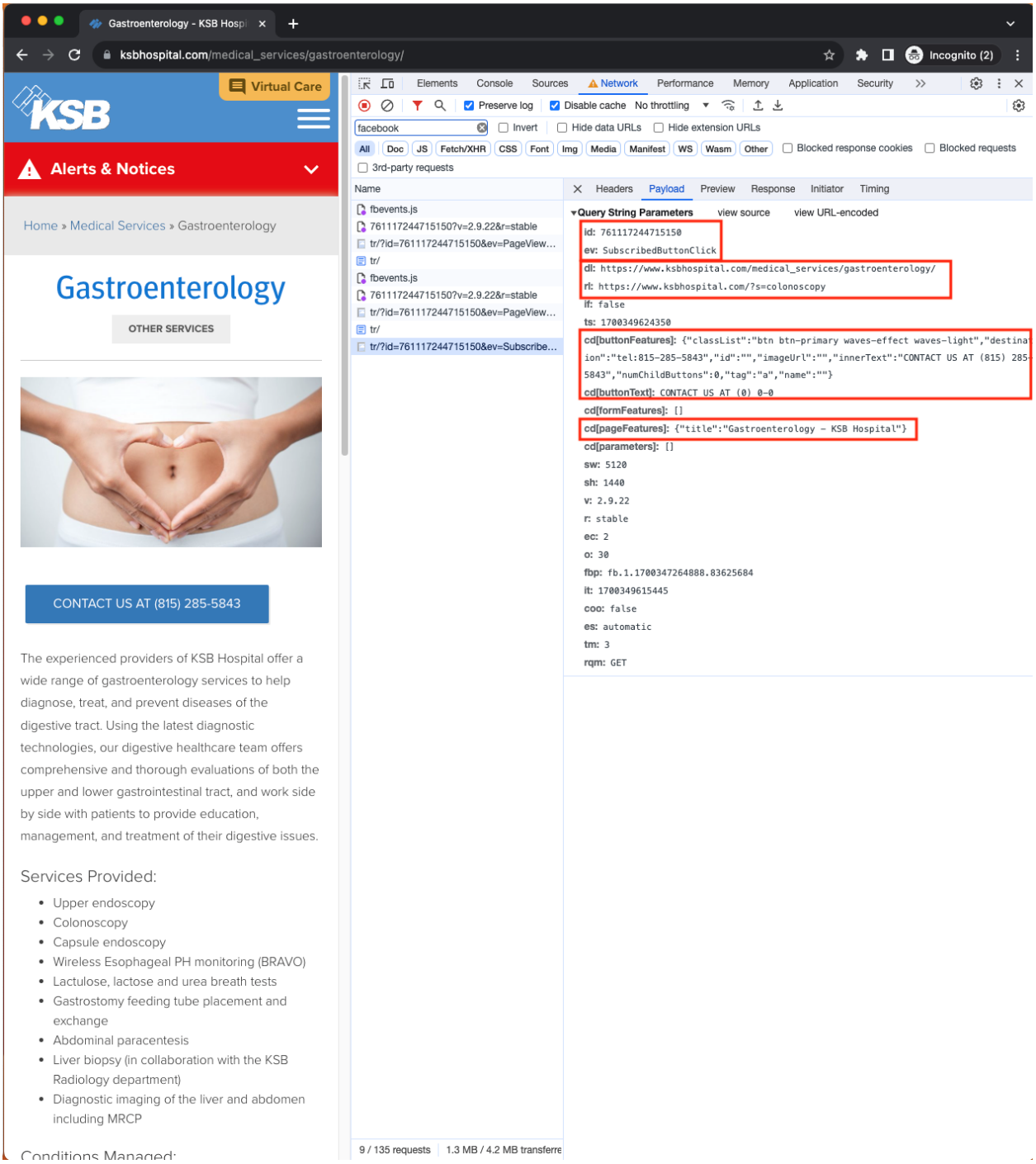
89. Upon a patient's arrival on the KSB homepage, KSB began its disclosures of patient activities by sending Facebook PageView and Microdata events. The events inform Facebook that the patient was on "https://www.ksbhospital.com/", a page about the "Katherine Shaw Bethea Hospital – KSB – Dixon, Illinois." *Id.*

90. Then, as the patient moved from the homepage to conduct a search for "colonoscopy," KSB reported that activity via a pair of PageView and Microdata events.. The Microdata event informs Facebook that the patient "searched for colonoscopy" on KSB's webpage.

91. KSB continued to inform Facebook as the patient navigated through their colonoscopy search results.

92. For example, when the patient loaded a page about gastroenterology, KSB transmitted PageView and Microdata events, which divulge the patient was on a page about "medical services/gastroenterology" after conducting a search for "colonoscopy."

93. KSB further disclosed through a SubscribedButtonClick event when the patient clicked the "CONTACT US" button to call KSB. The event disclosed that the patient clicked to call KSB from the "medical_services/gastroenterology" page after searching for "colonoscopy," as shown below:



KSB Disclosed Content That Patients Browsed

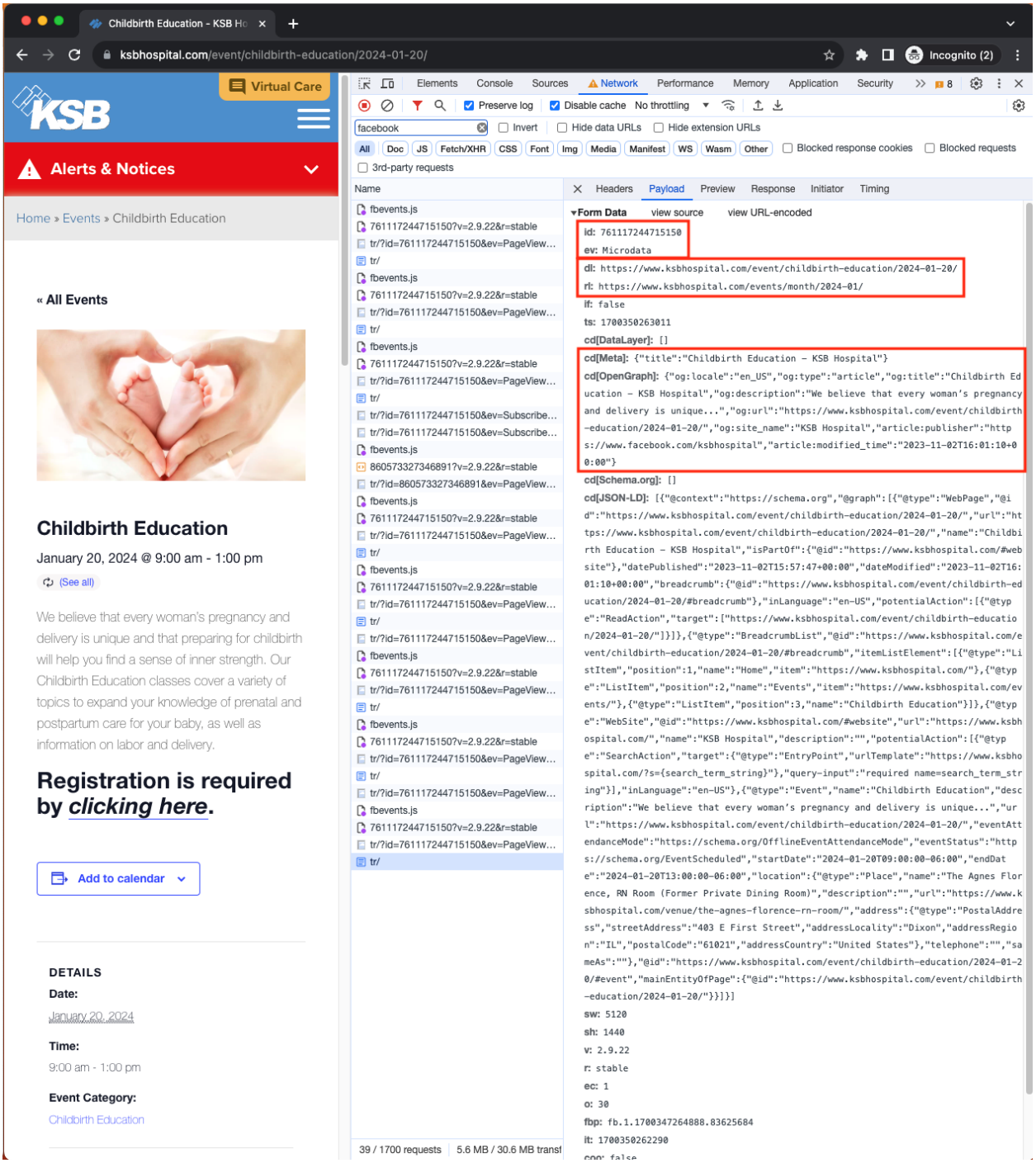
94. In addition to information about patients' search activities, KSB also disclosed to Facebook information about other types of browsing activities on KSB's website.

95. One example of patient browsing activity is the review of and registration for

classes KSB offered. As a patient navigated through KSB's website to view events, learn more about childbirth classes, and signed up for a class, KSB shared these activities with Facebook.

96. First, upon a patient visiting KSB's events page, KSB sent PageView and Microdata events to Facebook. The Microdata event divulges that the patient was viewing KSB's "Events from November 14 – April 25, 2024."

97. Next, KSB disclosed as the patient clicked on a specific class of interest. For example, when the patient clicked to view a Childbirth Education class, KSB transmitted PageView and Microdata events. The Microdata event informs Facebook both the name of the class, "Childbirth Education – KSB Hospital," as well as the date of the class, "2024-01-20/," as shown below:



98. KSB then disclosed when the patient selected the course. When the patient clicked to add the Childbirth Education class to their calendar, KSB sent a SubscribedButtonClick event, informing Facebook the patient clicked a button labeled "Add to Calendar" while they were on the page for "event/childbirth-education/2024-01-20/."

99. After the patient clicked to add the class to their calendar, KSB routed the user to a different website, Eventbrite.com. From there, the patient could complete the registration for KSB's course. The details of the user's Eventbrite.com activities were disclosed by Eventbrite to Facebook while the patient completed their registration for KSB's course.

100. Upon the patient loading the Eventbrite page, a PageView event was transmitted. Then, when the patient clicked to sign up for the class, a SubscribedButtonClick was sent revealing the user selected "KSB Childbirth Education Class" to obtain "ksb-childbirth-education-class-tickets." As the patient navigated to view the class details, clicked to get tickets, submitted their contact information, and finalized their registration, Eventbrite disclosed each of those activities through SubscribedButtonClick, PageView, and/or Microdata events.

101. Certain of Eventbrite's transmitted events revealed a substantial amount of information about the patient. For example, when the patient initially clicked to get tickets for the class, the SubscribedButtonClick event that was sent discloses that the patient chose to get the "KSB Childbirth Education Class Tickets, Sat, Jan 20, 2024 at 9:00 AM.". Moreover, Eventbrite had Advanced Matching Parameters enabled, and sent hashed versions of the user's entered first name, last name, email, phone number, city, zip code, and external ID in certain of the transmitted events.

KSB Disclosed Patients' Financial Related Activities

102. KSB additionally shared information about patients' financial related activities.

103. For example, KSB reported about patient bill pay activities as soon as the patient clicked to pay their bill online, upon which KSB transmitted a SubscribedButtonClick event. The SubscribedButtonClick event reveals the patient clicked to "PAY MY BILL ONLINE" on the page, "Financial Services – KSB Hospital."

104. As the patient navigated through KSB's instructions to pay their bill, KSB disclosed each one of those steps through a series of PageView, Microdata, and SubscribedButtonClick events.

105. First, when the patient arrived on KSB's bill pay page, KSB transmitted as set of PageView and Microdata events to disclose that activity.

106. From the bill pay page, the patient had the option of clicking to pay their medical bill or learning more about their healthcare bill. When the patient clicked to pay their bill, KSB disclosed that by sending a SubscribedButtonClick, which confirmed the patient clicked to "PAY YOUR MEDICAL BILL."

107. Next, KSB confirmed when the patient arrived on the page where they can pay their bill online by sending a pair of PageView and Microdata events, revealing the patient was on the page to "pay-your-medical-bill/." Finally, when the user clicked "Pay My Bill" to navigate to "https://www/personapay.com/ksb/login" KSB sent another SubscribedButtonClick event, informing Facebook the patient's click.

108. KSB also disclosed when patients conducted other financial activities.

109. For instance, when a patient clicked to estimate costs or to learn about financial assistance, KSB sent SubscribedButtonClick events for each activity. The SubscribedButtonClick events revealed that the patient clicked to either "ESTIMATE MY COST" or "LEARN ABOUT FINANCIAL ASSISTANCE," respectively.

110. In another example, when a patient viewed the Financial Assistance page, KSB sent PageView and Microdata events, confirming that the patient was on a page for "financial-services/financial-assistance."

KSB Disclosed Patients' Patient Portal and Medical Record Activities

111. Not only did KSB share information about patients' search, browsing, and financial activities, but KSB also sent information to Facebook about patients' activities revealing their status as potential patients.

112. One example of this type of activity is patient portal activities.

113. As soon as a patient loaded the page about the patient portal, KSB sent PageView and Microdata events, divulging that the patient was on the "Patient Portal – KSB Hospital" page where the patient can "Access your health records anytime."

114. When a patient clicked to log into the patient portal to use the health management tool, KSB sent a SubscribedButtonClick event. The SubscribedButtonClick event informs Facebook that the patient clicked "LOG IN" which leads to the URL: "https://ksb.iqhealth.com/."

115. Separately, KSB also shares when patients request medical records outside of the patient portal.

116. When a patient opened the Medical Records page, where the patient may either request a print or online version of a medical release authorization form, KSB sent a pair of PageView and Microdata events. The events divulge to Facebook that the patient was on a page about "medical-records/."

117. KSB then informed Facebook when the patient selected to either request the print or online version of the medical release authorization form.

118. If the patient clicked to access the print version of the form, KSB sent a SubscribedButtonClick informing Facebook the patient clicked "AUTHORIZATION FOR RELEASE OF MEDICAL INFROMATION – PRINTABLE FORM," which loads the file, "Release-of-Medical-Information-6_1_2023.pdf."

119. Similarly, when the patient opened the page with the online version of the

authorization form, KSB informed Facebook about that too. The PageView and Microdata events KSB sent revealed that the patient was on a page for "medical-records/online-roi-form" where the patient can make an "Online Request of Medical Record Information" if the user "complete[d] the below form to request your Medical Information."

120. Finally, when the patient submitted the online authorization form, KSB informed Facebook about that too, by sending a SubscribedButtonClick event confirming that the patient clicked to "Submit" a form for "medical-records/online-roi-form/."

121. After receiving this information from Defendant, Facebook processes it, analyzes it, and assimilates it into its own massive datasets, before selling access to this data in the form of targeted advertisements. Employing "Audiences"—subsections of individuals identified as sharing common traits—Facebook promises the ability to "find the people most likely to respond to your ad."[49] Advertisers can purchase the ability to target their ads based on a variety of criteria: "Core Audiences," individuals who share a location, age, gender, and/or language;[50] "Custom Audiences," individuals who have taken a certain action, such as visiting a website, using an app, or buying a product bought a product;[51] and/or "Lookalike Audiences," groups of individuals who "resemble" a Custom Audience, and who, as Facebook promises, "are likely to be interested in your business because they're similar to your best existing customers.[52]

122. Defendant could have chosen not to use the Meta Pixel, or it could have configured it to limit the information that it communicated to Facebook, but it did not. Instead, it intentionally selected and took advantage of the features and functionality of the Pixel that resulted in the

[49] Audience Ad Targeting, Meta, https://www.facebook.com/business/ads/ad-targeting
[50] *Id.*
[51] *Id.*
[52] How to Create a Lookalike Audience on Meta Ads Manager, Meta Business Help Center, https://www.facebook.com/business/help/465262276878947

Disclosure of Plaintiffs' and Class Members' Private Information.

123. Defendant used and disclosed Plaintiffs' and Class Members' Private Information to Facebook, Google, Innovid, CallRail, and possibly other third parties for the purpose of marketing its services and increasing its profits.

124. On information and belief, Defendant shared, traded, or sold Plaintiffs' and Class Members' Private Information with Facebook and others in exchange for improved targeting and marketing services and reduced marketing costs.

125. Plaintiffs never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information for marketing purposes. Plaintiffs were never provided with any written notice that Defendant regularly disclosed its patients' Protected Health Information to Facebook Google, Innovid, and CallRail, nor were they provided any means of opting out of such disclosures. Defendant, nonetheless, knowingly disclosed Plaintiffs' Protected Health Information to unauthorized entities and used that information for its own gain.

126. Plaintiffs and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for legitimate healthcare purposes only, and to make only authorized disclosures of this information.

127. Defendant actively misrepresented that it would preserve the security and privacy of Plaintiffs' and Class Members' Private Information. In actuality, Defendant shared data about Plaintiffs' and Class Members' activities on the Online Platforms alongside identifying details about the Plaintiffs and Class Members, such as their IP addresses.

128. By law, Plaintiffs and the Class Members are entitled to privacy in their Protected Health Information and confidential communications. KSB deprived Plaintiffs and Class Members of their privacy rights when it (1) implemented a system that surreptitiously tracked, recorded, and

disclosed Plaintiffs' and Class Members' confidential communications, Personally Identifiable Information, and Protected Health Information; (2) disclosed patients' Private Information to unauthorized, third-party eavesdroppers, including Facebook and others; (3) profited from the Disclosure; and (4) undertook this pattern of conduct without notifying Plaintiffs and Class Members and without obtaining their express written consent.

B. Plaintiffs' Experiences

Plaintiff Chloe Notftz's Experience

129. Plaintiff Chloe Noftz is a patient of Defendant and received healthcare services from KSB and physicians in KSB's network, specifically at the Dixon, Illinois location. She relied on KSB's Online Platforms to communicate confidential patient information.

130. Plaintiff Noftz has been a Facebook user for at least three years.

131. Plaintiff Noftz accessed Defendant's Online Platforms at Defendant's direction and encouragement. Plaintiff Noftz reasonably expected that her online communications with KSB were confidential, solely between herself and KSB, and that, as such, those communications would not be transmitted to or intercepted by a third party.

132. Plaintiff Noftz utilized and accessed Defendant's Online Platforms in order to manage her treatment for a broken toe. Plaintiff Noftz would regularly use Defendant's Online Platforms to check medical bills and to view different test results.

133. Following Plaintiff Noftz's use of Defendant's Online Platforms, she noticed that she was receiving targeted ads regarding Defendant's health plans. This caused Plaintiff Noftz some concern and she refused to utilize Defendant's Online Platforms following the targeted ads appearing on Facebook.

134. Plaintiff Noftz provided her Private Information to Defendant and trusted that the

information would be safeguarded according to KSB's privacy policies and the law.

135. As described herein, by use of the Meta Pixel and tracking technology, KSB sent Plaintiff Noftz's Private Information to Facebook and others when she used Defendant's Online Platforms to communicate healthcare and identifying information to KSB.

136. Pursuant to the process described herein, KSB assisted Facebook and potentially others in intercepting Plaintiff Noftz's confidential communications, including those that contained PII and PHI. KSB facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization.

137. Plaintiff never intended to sell her Private Information or would have permitted it to be made available for sale on the resale market.

138. On information and belief, through its use of the Meta Pixel and other tracking technologies, KSB disclosed to Facebook:

a. The pages and content Plaintiff viewed;

b. Plaintiff's seeking of medical treatment;

c. Plaintiff's status as a patient;

d. Information regarding Plaintiff's patient portal activity;

e. The specialties of the medical providers Plaintiff searched for and viewed;

f. the names of the medical providers Plaintiff searched for and viewed;

g. the search results that Plaintiff clicked on;

h. the medical services Plaintiff viewed; and,

i. Plaintiff's identity via her IP address and/or "c_user" cookie and/or Facebook ID.

139. By failing to receive the requisite consent, KSB breached confidentiality and unlawfully disclosed Plaintiff's Private Information.

140. As a result of KSB's Disclosure of Plaintiff's Private Information via the Meta Pixel and other tracking technologies to third parties without authorization, Plaintiff has suffered the following injuries:

a. Loss of privacy; unauthorized disclosure of her Private Information; unauthorized access of her Private Information by third parties;

b. Plaintiff now receives targeted health-related advertisements on Facebook, reflecting her private medical treatment information;

c. Plaintiff paid KSB for medical services and the services she paid for included reasonable privacy and data security protections for her Private Information, but Plaintiff did not receive the privacy and security protections for which she paid, due to Defendant's Disclosure;

d. The portion of KSB's revenues and profits attributable to collecting Plaintiff's Private Information without authorization and sharing it with third parties;

e. The portion of KSB's savings in marketing costs attributable to collecting Plaintiff's Private Information without authorization and sharing it with third parties;

f. The portion of KSB's revenues and profits attributable to serving and monetizing advertisements directed to Plaintiff as a result of collecting Plaintiff's Private Information without authorization and sharing it with third parties;

g. Value to Plaintiff of surrendering her choice to keep her Private Information private and allowing KSB to track her data;

h. Embarrassment, humiliation, frustration, and emotional distress;

i. Decreased value of Plaintiff's Private Information;

j. Lost benefit of the bargain;

k. Increased risk of future harm resulting from future use and disclosure of her Private Information; and

l. Statutory damages.

Plaintiff Tonya Black's Experience

141. Plaintiff Tonya Black is a patient of Defendant and received healthcare services from KSB and physicians in KSB's network, specifically an OBGYN in a KSB hospital. She relied on KSB's Online Platforms to communicate confidential patient information.

142. Plaintiff has been a Facebook user for eight years.

143. Plaintiff Black accessed Defendant's Online Platforms at Defendant's direction and encouragement. Plaintiff Black reasonably expected that her online communications with KSB were confidential, solely between herself and KSB, and that, as such, those communications would not be transmitted to or intercepted by a third party.

144. Plaintiff Black utilized and accessed Defendant's patient portal for a variety of reasons – to view test results, schedule appointments, and track her prescriptions. Additionally, Plaintiff Black utilized Defendant's website to locate phone numbers for her OBGYN and primary care doctor.

145. Plaintiff Black provided her Private Information to Defendant and trusted that the information would be safeguarded according to KSB's privacy policies and legal obligations.

146. As described herein, by use of the Meta Pixel and tracking technology, KSB sent Black's Private Information to Facebook and others when she used Defendant's Online Platforms to communicate healthcare and identifying information to KSB.

147. Pursuant to the process described herein, KSB assisted Facebook and others with

intercepting Plaintiff Black's confidential communications, including those that contained PII and PHI. KSB facilitated these interceptions without Plaintiffs' knowledge, consent, or express written authorization.

148. Plaintiff never intended to sell her Private Information or would have permitted it to be made available for sale on the resale market.

149. On information and belief, through its use of the Meta Pixel and other tracking technologies, KSB disclosed to Facebook:

a. The pages and content Plaintiff viewed;

b. Plaintiff's seeking of medical treatment;

c. Plaintiff's status as a patient;

d. Information regarding Plaintiff's patient portal activity;

e. The specialties of the medical providers Plaintiff searched for and viewed;

f. the names of the medical providers Plaintiff searched for and viewed;

g. the search results that Plaintiff clicked on;

h. the medical services Plaintiff viewed; and,

i. Plaintiff's identity via her IP address and/or "c_user" cookie and/or Facebook ID.

150. By failing to receive the requisite consent, KSB breached confidentiality and unlawfully disclosed Plaintiff's Private Information.

151. As a result of KSB's Disclosure of Plaintiff's Private Information via the Meta Pixel and other tracking technologies to third parties without authorization, Plaintiff has suffered the following injuries:

a. Loss of privacy; unauthorized disclosure of her Private Information; unauthorized access of her Private Information by third parties;

b. Plaintiff now receives targeted health-related advertisements on Facebook, reflecting her private medical treatment information;

c. Plaintiff paid KSB for medical services and the services she paid for included reasonable privacy and data security protections for her Private Information, but Plaintiff did not receive the privacy and security protections for which she paid, due to Defendant's Disclosure;

d. The portion of KSB's revenues and profits attributable to collecting Plaintiff's Private Information without authorization and sharing it with third parties;

e. The portion of KSB's savings in marketing costs attributable to collecting Plaintiff's Private Information without authorization and sharing it with third parties;

f. The portion of KSB's revenues and profits attributable to serving and monetizing advertisements directed to Plaintiff as a result of collecting Plaintiff's Private Information without authorization and sharing it with third parties;

g. Value to Plaintiff of surrendering her choice to keep her Private Information private and allowing KSB to track her data;

h. Embarrassment, humiliation, frustration, and emotional distress;

i. Decreased value of Plaintiff's Private Information;

j. Lost benefit of the bargain;

k. Increased risk of future harm resulting from future use and disclosure of her Private Information; and

l. Statutory damages.

Plaintiff Kenneth Weinstock's Experience

152. Plaintiff Kenneth Weinstock is a patient of Defendant and received healthcare services from KSB and physicians in KSB's network, particularly at KSB Commerce Towers, KSB Hennapan, and a KSB emergency department. He relied on KSB's Online Platforms to communicate confidential patient information.

153. Plaintiff Weinstock has been a Facebook user since 2018.

154. Plaintiff Weinstock accessed Defendant's Online Platforms at Defendant's direction and encouragement. Plaintiff Weinstock reasonably expected that his online communications with KSB were confidential, solely between himself and KSB, and that, as such, those communications would not be transmitted to or intercepted by a third party.

155. Plaintiff Weinstock utilized and accessed Defendant's patient portal to manage a variety of treatments for kidney stones, his physical therapy appointments, and general pain management. Plaintiff Weinstock also used Defendant's patient portal to view test results and appointment times. Plaintiff Weinstock also accessed Defendant's website to find a primary care doctor, hours of operations of different KSB locations, and leave reviews.

156. Following Plaintiffs' use of Defendant's Online Platforms, he began to notice targeted ads for KSB hospitals' pain management classes.

157. Plaintiff Weinstock provided his Private Information to Defendant and trusted that the information would be safeguarded according to KSB's privacy policies and legal obligations.

158. As described herein, by use of the Meta Pixel and tracking technology, KSB sent Weinstock's Private Information to Facebook and others when he used Defendant's Online Platforms to communicate healthcare and identifying information to KSB.

159. Pursuant to the process described herein, KSB assisted Facebook and others with

intercepting Plaintiff Weinstock's confidential communications, including those that contained PII and PHI. KSB facilitated these interceptions without Plaintiffs' knowledge, consent, or express written authorization.

160. Plaintiff never intended to sell his Private Information or would have permitted it to be made available for sale on the resale market.

161. On information and belief, through its use of the Meta Pixel and other tracking technologies, KSB disclosed to Facebook:

a. The pages and content Plaintiff viewed;

b. Plaintiff's seeking of medical treatment;

c. Plaintiff's status as a patient;

d. Information regarding Plaintiff's patient portal activity;

e. The specialties of the medical providers Plaintiff searched for and viewed;

f. the names of the medical providers Plaintiff searched for and viewed;

g. the search results that Plaintiff clicked on;

h. the medical services Plaintiff viewed; and,

i. Plaintiff's identity via his IP address and/or "c_user" cookie and/or Facebook ID.

162. By failing to receive the requisite consent, KSB breached confidentiality and unlawfully disclosed Plaintiff's Private Information.

163. As a result of KSB's Disclosure of Plaintiff's Private Information via the Meta Pixel and other tracking technologies to third parties without authorization, Plaintiff has suffered the following injuries:

a. Loss of privacy; unauthorized disclosure of his Private Information; unauthorized access of his Private Information by third parties;

b. Plaintiff now receives targeted health-related advertisements on Facebook, reflecting his private medical treatment information;

c. Plaintiff paid KSB for medical services and the services he paid for included reasonable privacy and data security protections for his Private Information, but Plaintiff did not receive the privacy and security protections for which he paid, due to Defendant's Disclosure;

d. The portion of KSB's revenues and profits attributable to collecting Plaintiff's Private Information without authorization and sharing it with third parties;

e. The portion of KSB's savings in marketing costs attributable to collecting Plaintiff's Private Information without authorization and sharing it with third parties;

f. The portion of KSB's revenues and profits attributable to serving and monetizing advertisements directed to Plaintiff as a result of collecting Plaintiff's Private Information without authorization and sharing it with third parties;

g. Value to Plaintiff of surrendering her choice to keep his Private Information private and allowing KSB to track his data;

h. Embarrassment, humiliation, frustration, and emotional distress;

i. Decreased value of Plaintiff's Private Information;

j. Lost benefit of the bargain;

k. Increased risk of future harm resulting from future use and disclosure of her Private Information; and

l. Statutory damages.

C. Investigations and Reports Reveal the Meta Pixel's Impermissible Collection of PHI

164. In June 2020, after promising users that app developers would not have access to data if users were not active in the prior 90 days, Facebook revealed that it still enabled third-party developers to access this data.[53] This failure to protect users' data enabled thousands of developers to see data on inactive users' accounts if those users were Facebook friends with someone who was an active user.

165. On February 18, 2021, the New York State Department of Financial Services released a report detailing the significant privacy concerns associated with Facebook's data collection practices, including the collection of health data. The report noted that while Facebook maintained a policy that instructed developers not to transmit sensitive medical information, Facebook received, stored, and analyzed this information anyway. The report concluded that "[t]he information provided by Facebook has made it clear that Facebook's internal controls on this issue have been very limited and were not effective . . . at preventing the receipt of sensitive data."[54]

166. The New York State Department of Financial Service's concern about Facebook's cavalier treatment of private medical data was not misplaced. In June 2022, the FTC finalized a different settlement involving Facebook's monetizing of sensitive medical data. In that case, the more than 100 million users of Flo, a period and ovulation tracking app, learned something startling: the company was sharing their data with Facebook.[55] When a user was having her period or informed the app of her intention to get pregnant, Flo would inform Facebook, which could then

[53] Kurt Wagner & Bloomberg, Facebook Admits Another Blunder with User Data, FORTUNE (July 1, 2020 at 6:30 p.m.) https://fortune.com/2020/07/01/facebook-user-data-apps-blunder/.
[54] New York State Department of Financial Services, REPORT ON INVESTIGATION OF FACEBOOK INC. DATA PRIVACY CONCERNS, (Feb. 18, 2021) https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_20210218.pdf.
[55] Justin Sherman, Your Health Data Might Be for Sale, SLATE (June 22, 2022 at 5:50 a.m.) https://slate.com/technology/2022/06/health-data-brokers-privacy.html.

use the data for targeted advertising. In 2021, Flo settled with the Federal Trade Commission for lying to its users about its secret sharing their data with Facebook, as well as with a host of other internet advertisers, including Google, Fabric, AppsFlyer, and Flurry. The FTC reported that Flo "took no action to limit what these companies could do with users' information."[56]

167. More recently, Facebook employees admitted to lax protections for sensitive user data. In 2021, Facebook engineers on the ad business product team conceded "[w]e do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.'"[57]

168. In June 2022, an investigation by The Markup[58] revealed that 33 of the top 100 hospitals in the nation had the Meta Pixel embedded on their websites.[59] On those hospital websites, the Meta Pixel collects and sends Facebook a "packet of data" including sensitive personal health information whenever a user interacts with the website, for example, by clicking a button to schedule a doctor's appointment.[60] The data is connected to an IP address, which is "an identifier that's like a computer's mailing address and can generally be linked to a specific individual or household—creating an intimate receipt of the appointment request for Facebook."[61]

169. During its investigation, The Markup found that Facebook's purported "filtering"

---

[56] *Id.*
[57] Lorenzo Franceschi-Bicchierai, Facebook Doesn't Know What It Does with Your Data, or Where It Goes: Leaked Document, VICE (April 26, 2022) https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes.
[58] The Markup is a nonprofit newsroom that investigates how powerful institutions are using technology to change our society. *See* www.themarkup.org/about
[59] Todd Feathers, Simon Fondrie-Teitler, Angie Waller, & Surya Mattu, Facebook Is Receiving Sensitive Medical Information from Hospital Websites, THE MARKUP (June 16, 2022 6:00 a.m.) https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.
[60] *Id.*
[61] *Id.*

failed to discard even the most obvious forms of sexual health information. Worse, the article found that the data that the Meta Pixel was sending Facebook from hospital websites included patients' medications, descriptions of their allergic reactions, details about their upcoming doctor's appointments, and patients' names, addresses, email addresses, and phone numbers.[62]

170. In addition to the 33 hospitals identified by The Markup as having installed the Meta Pixel on their websites, The Markup identified seven health systems that had installed the Meta Pixel inside their password-protected patient portals.[63]

171. David Holtzman, health privacy consultant and former senior privacy adviser in the U.S. Department of Health and Human Services' Office for Civil Rights, stated he was "deeply troubled" by what the hospitals capturing and sharing patient data in this way.[64]

D. Defendant Violated HIPAA Standards

172. Under HIPAA, a healthcare provider may not disclose personally identifiable, non-public medical information (PHI) about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.[65]

173. Guidance from the U.S. Department of Health and Human Services ("HHS") instructs healthcare providers that patient status alone is protected by HIPAA.

174. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the Department instructs:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to

[62] *Id.*
[63] *Id.*
[64] *Id.*
[65] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

> health data… If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[66]

175. In its guidance for Marketing, the Department further instructs:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list. (Emphasis added).[67]

176. In addition, HHS's Office for Civil Rights (OCR) issued a Bulletin to highlight the obligations of HIPAA-covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technology.[68]

177. According to the Bulletin, "HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information."[69]

178. Citing The Markup's June 2022 article, the Bulletin expressly notes:

> Some regulated entities may share sensitive information with online tracking technology vendors and such sharing may be unauthorized disclosures of PHI with such vendors. **Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking**

---

[66] U.S. Department of Health and Human Services, Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, (Nov. 26, 2012) https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.

[67] U.S. Department of Health and Human Services, Marketing, (Dec. 3, 2002) https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf.

[68] *See* U.S. Department of Health and Human Services, Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, https://www.hhs.gov/hipaa/forprofessionals/privacy/guidance/hipaa-online-tracking/index.html.

[69] *Id.*

> **technology vendors or any other violations of the HIPAA Rules**. For example, disclosures of PHI to tracking technology vendors or marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.
>
> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI **only** as expressly permitted or required by the HIPAA Privacy Rule. [70]

179. In other words, HHS has expressly stated that Defendant's conduct of implementing the Meta Pixel violates HIPAA Rules.

E. Defendant Violated FTC Standards, and the FTC and HSS Take Action

180. The Federal Trade Commission ("FTC") has also recognized that implementation of the Meta Pixel and other tracking technologies pose "serious privacy and security risks" and "impermissibly disclos[e] consumers' sensitive personal health information to third parties."[71]

181. On July 20, 2023, the FTC and HHS sent a "joint letter to approximately 130 hospital systems and telehealth providers to alert them about the risks and concerns about the use of technologies, such as Meta/Facebook pixel and Google Analytics, that can track a user's online activities."[72]

---

[70] *Id.* (emphasis in original) (internal citations omitted).

[71] Re: Use of Online Tracking Technologies, U.S. Dep't of Health & Human Services, (July 20, 2023) (available at https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf), **attached as Exhibit A.**

[72] FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies, FEDERAL TRADE COMMISSION (July 20, 2023) https://www.ftc.gov/news-

182. Therein, the FTC reminded healthcare providers that "HIPAA regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to third parties or any other violations of the HIPAA Rules"[73] and that "[t]his is true even if you relied upon a third party to develop your website or mobile app and even if you do not use the information obtained through use of a tracking technology for any marketing purposes."[74]

183. Entities that are not covered by HIPAA also face accountability for disclosing consumers' sensitive health information under the Health Breach Notification Rule. 16 C.F.R. § 318. This Rule requires that companies dealing with health records notify the FTC and consumers if there has been a breach of unsecured identifiable health information, or else face civil penalties for violations. *Id*. According to the FTC, "a 'breach' is not limited to cybersecurity intrusions or nefarious behavior. Incidents of unauthorized access, *including sharing of covered information without an individual's authorization*, triggers notification obligations under the Rule."[75]

184. Additionally, the FTC Act makes it unlawful to employ "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce[.]" 15 U.S.C. § 45(a). According to the FTC, "the disclosure of [sensitive health] information without a consumer's authorization can, in some circumstances, violate the FTC Act

events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking?utm_source=govdelivery.

[73] *Id.*

[74] *Id.*

[75] Statement of the Commission: On Breaches by Health Apps and Other Connected Devices, U.S. Fed. Trade Commission, (Sept. 15, 2021) (available at https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf) (emphasis added).

as well as constitute a breach of security under the FTC's Health Breach Notification Rule."[76]

185. As such, the FTC and HHS have expressly stated that conduct like Defendant's runs afoul of the FTC Act and/or the FTC's Health Breach Notification Rule.

F. Defendant Violated Industry Standards

186. A medical provider's duty of confidentiality is a cardinal rule, embedded in doctor-patient and hospital-patient relationships.

187. The American Medical Association's ("AMA") Code of Medical Ethics requires the protection of patient privacy and communications, and these rules are applicable to KSB and its physicians.

188. AMA Code of Ethics Opinion 3.1.1 provides:

> Protecting information gathered in association with the care of the patient is a core value in health care . . . . Patient privacy encompasses a number of aspects, including . . . personal data (informational privacy).

189. AMA Code of Medical Ethics Opinion 3.2.4 provides:

> Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (a) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

[76] *See, e.g.,* U.S. v. Easy Healthcare Corp., Case No. 1:23-cv-3107 (N.D. Ill. 2023), https://www.ftc.gov/legallibrary/browse/cases-proceedings/202-3186-easy-healthcare-corporation-us-v; In the Matter of BetterHelp, Inc., FTC Dkt. No. C-4796 (July 14, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc-matter; U.S. v. GoodRx Holdings, Inc., Case No. 23-cv-460 (N.D. Cal. 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc; In the Matter of Flo Health Inc., FTC Dkt. No. C-4747 (June 22, 2021), https://www.ftc.gov/legal-library/browse/casesproceedings/192-3133-flo-health-inc.

190. AMA Code of Medical Ethics Opinion 3.3.2 provides:

> Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically . . . must . . . release patient information only in keeping ethics guidelines for confidentiality.

G. Defendant Violated Standards Set Forth in Illinois Law

191. Under the Illinois Medical Patient Rights Act ("MPRA"), 410 Ill. Comp. Stat. 50/3(d), Plaintiff and Class Members have rights to privacy and confidentiality in their health care.

192. The MPRA provides:

> Each physician, health care provider, health services corporation and insurance company shall refrain from disclosing the nature or details of services provided to patients, except that such information may be disclosed: (1) to the patient, (2) to the party making treatment decisions if the patient is incapable of making decisions regarding the health services provided, (3) for treatment in accordance with 45 CFR 164.501 and 164.506, (4) for payment in accordance with 45 CFR 164.501 and 164.506, (5) to those parties responsible for peer review, utilization review, and quality assurance, (6) for health care operations in accordance with 45 CFR 164.501 and 164.506, (7) to those parties required to be notified under the Abused and Neglected Child Reporting Act or the Illinois Sexually Transmissible Disease Control Act, or (8) as otherwise permitted, authorized, or required by State or federal law. This right may be waived in writing by the patient or the patient's guardian or legal representative, but a physician or other health care provider may not condition the provision of services on the patient's, guardian's, or legal representative's agreement to sign such a waiver.

410 Ill. Comp. Stat. 50/3(d).

193. Furthermore, the Illinois Personal Information Protection Act ("IPIPA") protects Plaintiffs' and Class Members' Medical Information and Personal Information from unauthorized disclosure. 815 Ill. Comp. Stat. 530/5, /45.

194. Defendant is a "Data Collector" and subject to the provisions of the IPIPA. *See* 815 Ill. Comp. Stat. 530/5.

195. The IPIPA provides that:

> A data collector that owns or licenses, or maintains or stores but does not own or

> license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

815 Ill. Comp. Stat. 530/459(a).

196. Defendant's Disclosure of Plaintiffs' and Class Members' Private Information to third parties, including Facebook, Google, and DoubleClick, the Trade Desk, Frequence and possibly others, through the operation of the Pixel on its Website and Online Platforms violated Plaintiffs' and Class Members' rights to privacy and confidentiality in their receipt of healthcare services and fell below the applicable standard for safeguarding the confidential Private Information of Plaintiff and the Class Members.

H. Plaintiffs' and Class Members' Expectation of Privacy

197. At all times when Plaintiffs and Class Members provided their Private Information to Defendant, they had a reasonable expectation that the information would remain private and that Defendant would not share the Private Information with third parties for a commercial marketing and sales purposes, unrelated to patient care.

I. IP Addresses are Personally Identifiable Information

198. Defendant also disclosed Plaintiffs' and Class Members' IP addresses to Facebook and others through its use of the Meta Pixel and other tracking technologies.

199. An IP address is a number that identifies the address of a device connected to the Internet.

200. IP addresses are used to identify and route communications on the Internet.

201. IP addresses of individual Internet users are used by Internet service providers, Websites, and third-party trackers to facilitate and track Internet communications.

202. Facebook tracks every IP address ever associated with a Facebook user.

203. Facebook tracks IP addresses for use of targeting individual homes and their occupants with advertising.

204. Under HIPAA, an IP address is Personally Identifiable Information:

- HIPAA defines personally identifiable information to include "any unique identifying number, characteristic or code," specifically listing IP addresses as an example of PII. *See* 45 C.F.R. § 164.514 (2).

- HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *See also*, 45 C.F.R. § 164.514(b)(2)(i)(O).

205. Consequently, by disclosing IP addresses, Defendant's business practices violated HIPAA and industry privacy standards.

J. Defendant Was Enriched by and Benefitted from the Use of Plaintiffs' and Class Members' Private Information

206. The sole purpose for Defendant's use of the Meta Pixel and other tracking technology was to enhance its marketing efforts and increase its profits.

207. In exchange for disclosing the Private Information of its patients, Defendant was compensated by Facebook and likely others in the form of enhanced advertising services and more cost-efficient marketing.

208. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients.

209. By utilizing the Meta Pixel and other trackers, the cost of advertising and retargeting was reduced, thereby benefiting Defendant.

K. Plaintiffs' and Class Members' Private Information Had Financial Value

210. The data concerning Plaintiffs' and Class Members, collected and shared by

Defendant, has tremendous economic value. Data collected via the Meta Pixel, CAPI, and other online tracking tools allows Facebook to build its own massive, proprietary dataset, to which it then sells access in the form of targeted advertisements. Targeting works by allowing advertisers to direct their ads at particular "Audiences," subsets of individuals who, according to Facebook, are the "people most likely to respond to your ad."[77] Facebook's "Core Audiences" allow advertisers to target individuals based on demographics, such as age, location, gender, or language, whereas "Custom Audiences" allow advertisers to target individuals who have "already shown interest in your business," by visiting a business's website, using an app, or engaging in certain online content.[78] Facebook's "Lookalike Audiences" go further, targeting individuals who resemble current customer profiles and whom, according to Facebook, "are likely to be interested in your business."[79]

211. Plaintiffs had a recognizable property interest in their browsing history. That browsing history has economic value, and by sharing, or facilitating the sharing of, such information with third parties such as Google and Facebook without prior approval, KSB took something of value from Plaintiffs and provided it to third parties without compensating Plaintiffs for the use of their Private Information and data, thus, causing the Plaintiffs economic injury.

212. Plaintiffs' Private Information, which was taken by Defendant without permission, had value even though it was not "for sale." The browsing history and data mined from individuals using the internet has significant economic value. If it did not have value, then entire industries that sell and trade this data would not exist. There is an entire data industry and estimates suggests that that industry generates billions of dollars.

---

[77] Audience Ad Targeting, Meta, https://www.facebook.com/business/ads/ad-targeting
[78] *Id.*
[79] *See* How to Create a Lookalike Audience on Meta Ads Manager, Meta Business Center, https://www.facebook.com/business/help/465262276878947

213. Data harvesting is big business, and it drives Facebook's profit center, its advertising sales. In 2019, Facebook generated nearly $70 billion dollars in advertising revenue alone, constituting more than 98% of its total revenue for that year.[80]

214. This business model is not limited to Facebook. Data harvesting one of the fastest growing industries in the country, and consumer data is so valuable that it has been described as the "new oil." Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure is only due to keep increasing; estimates for 2022 were as high as $434 per user, for a total of more than $200 billion industry wide.

215. In particular, the value of health data is well-known due to the media's extensive reporting on the subject. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry." Therein, it described the extensive market for health data and observed that the health data market is both lucrative and a significant risk to privacy.[81]

216. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[82]

TOLLING, CONCEALMENT, AND ESTOPPEL

217. The applicable statutes of limitation have been tolled as a result of KSB's knowing and active concealment and denial of the facts alleged herein.

---

[80] *See* Here's How Big Facebook's Ad Business Really Is, CNN, https://www.cnn.com/2020/06/30/tech/facebook-ad-business-boycott/index.html

[81] *See* Adam Tanner, How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry, TIME, (Jan. 9, 2017 at 9:00 a.m.) https://time.com/4588104/medical-data-industry/.

[82] *See* Christina Farr, Hospital Execs Say They are Getting Flooded with Requests for Your Health Data, CNBC, (Dec. 18, 2019 at 8:27 a.m.) https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html.

218. KSB seamlessly incorporated Meta Pixel and other trackers into its Website and Online Platforms while providing patients with no indication that their Website usage was being tracked and transmitted to third parties. KSB knew that its Website incorporated Meta Pixel and other trackers, yet it failed to disclose to Plaintiffs and Class Members that their sensitive medical information would be intercepted, collected, used by, and disclosed to Facebook.

219. Even while exercising due diligence, Plaintiffs and Class Members could not have discovered the full scope of KSB's conduct, because there were no disclosures or other indications that they were interacting with websites employing Meta Pixel or any other tracking technology.

220. All applicable statutes of limitation have also been tolled by operation of the discovery rule and the doctrine of continuing tort. KSB's illegal interception and disclosure of Plaintiffs' Private Information has continued unabated through the present. What is more, KSB was under a duty to disclose the nature and significance of their data collection practices but did not do so. KSB is therefore, is estopped from relying on any statute of limitations defenses.

CLASS ACTION ALLEGATIONS

221. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of other similarly situated persons.

222. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> **All patients of Defendant whose Private Information was disclosed by Defendant to third parties through the Meta Pixel and related technology without authorization.**

223. Further, Plaintiffs seek to represent an Illinois Subclass, defined as:

> **All patients of Defendant who are Illinois citizens and whose Private Information was disclosed by Defendant to third parties through the Meta Pixel and related technology without authorization.**

224. The Nationwide Class and Illinois Subclass are collectively referred to as "the

Class."

225. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers, and directors, and any entity in which Defendant have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state, or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels, and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

226. Plaintiffs reserve the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

227. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23(a)(1)-(4).

228. Numerosity: Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are hundreds or thousands of individuals whose Private Information may have been improperly accessed in the Disclosure, and each Class is apparently identifiable within Defendant's records.

229. Commonality: Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include

a. whether and to what extent Defendant had a duty to protect Plaintiffs' and Class Members' Private Information;

b. whether Defendant had duties not to disclose the Plaintiffs' and Class Members' Private Information to unauthorized third parties;

c. whether Defendant had duties not to use Plaintiffs' and Class Members' Private

Information for non-healthcare purposes;

d. whether Defendant had duties not to use Plaintiffs' and Class Members' Private Information for unauthorized purposes;

e. whether Defendant failed to adequately Plaintiffs' and Class Members' Private Information;

f. whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

g. whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

h. whether Defendant failed to properly implement and configure the tracking software on its Online Platforms to prevent the disclosure of confidential communications and Private Information;

i. whether Defendant's conduct breached its duties of care and amounts to negligence;

j. whether Defendant was negligent *per se*;

k. whether Defendant breached its implied contract with Plaintiffs and the Class Members; or in the alternate, whether Defendant was unjustly enriched;

l. whether Defendant's conduct violated the Illinois Eavesdropping Statute, 720 Ill. Comp. Stat. 5/14, *et seq*.;

m. whether Defendant's conduct violated the Electronic Communications Privacy Act, 18 U.S.C. §§ 2511(1), *et seq.*;

n. whether Defendant's conduct violated the Electronic Communications Privacy Act, 18 U.S.C. § 2511(3)(a) ("Unauthorized Divulgence By Electronic Communications Service");

o. whether Defendant's conduct violated Title II of the Electronic Communications Privacy Act, 18 U.S.C. § 2702, *et seq*.;

p. whether Defendant's conduct violated the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, *et seq.*

q. whether Plaintiffs and the Class Members are entitled to damages, including actual, compensatory, and nominal damages;

r. the measure of Plaintiffs' and the Class Members' damages; and,

s. whether Plaintiffs and the Class Members are entitled to punitive damages

230. Typicality: Plaintiffs' claims are typical of those of other Class Members because all had their Private Information compromised as a result of Defendant's use and incorporation of Meta Pixel and other tracking technology.

231. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant have acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly, and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

232. Adequacy: Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages Plaintiffs have suffered is typical of other Class Members. Plaintiffs have also retained counsel experienced in

complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

233. Superiority and Manageability: Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

234. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged. If the class action device were not used, Defendant would necessarily gain an unconscionable advantage because they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources. Moreover, the costs of individual suits could unreasonably consume the amounts that would be recovered, whereas proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged. Finally, individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

235. The litigation of the claims brought herein is manageable. Defendant's uniform

conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

236. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

237. Unless a Class-wide injunction is issued, Defendant may continue in their unlawful disclosure and failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding Disclosure, and Defendant may continue to act unlawfully as set forth in this Complaint.

238. Further, Defendant have acted or refused to act on grounds generally applicable to the Class, and, accordingly, final injunctive or corresponding declaratory relief regarding the whole of the Class is appropriate.

239. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to the following:

a. whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to the disclosure of patient information;

d. whether Defendant was negligent and/or negligent *per se*;

e. whether an implied contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that contract;

f. whether Defendant breached the contract;

g. in the alternate, whether Defendant was unjustly enriched;

h. whether Defendant adequately and accurately informed Plaintiffs and Class Members that their Private Information had been used and disclosed to third parties;

i. whether Defendant failed to implement and maintain reasonable security procedures and practices;

j. whether Defendant violated the Illinois Eavesdropping Statute, 720 Ill. Comp. Stat. 5/14, *et seq*.;

k. whether Defendant's conduct violated the Electronic Communications Privacy Act, 18 U.S.C. §§ 2511(1), *et seq.*;

l. whether Defendant's conduct violated the Electronic Communications Privacy Act, 18 U.S.C. § 2511(3)(a) ("Unauthorized Divulgence By Electronic Communications Service");

m. whether Defendant's conduct violated Title II of the Electronic Communications Privacy Act, 18 U.S.C. § 2702, *et seq*.;

n. whether Defendant's conduct violated the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, *et seq.*; and,

o. whether Plaintiffs and the Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

240. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

241. Defendant owed to Plaintiffs and Class Members a duty to exercise reasonable care in handling and using Plaintiffs' and Class Members' Private Information in its care and custody, including implementing industry-standard privacy procedures sufficient to reasonably protect the information from the disclosure and unauthorized transmittal and use of Private Information that occurred.

242. Defendant acted with wanton and reckless disregard for the privacy and confidentiality of Plaintiffs' and Class Members' Private Information by disclosing and providing access to this information to third parties for the financial benefit of the third parties and Defendant.

243. Defendant owed these duties to Plaintiffs and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's disclosure of their Private Information to benefit third parties and Defendant. Defendant actively sought and obtained Plaintiffs' and Class Members' Private Information.

244. Defendant's duty arose as a result of industry standards and the physician-patient relationship to keep patient's Private Information, PHI and PII of Plaintiffs and the Class Members, gathered in that relationship secret; as well as due to Defendant collecting Private Information from patients online

245. Private Information is highly valuable, and Defendant knew, or should have known, the harm that would be inflicted on Plaintiffs and Class Members by disclosing their Private Information to third parties. This disclosure was of benefit to third parties and Defendant by way

of data harvesting, advertising, and increased sales.

246. Defendant breached its duties and was negligent by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers in the handling and securing of Private Information of Plaintiffs and Class Members, and by failing to disclose Defendant was gathering Private Information, including PHI and PII, and sharing it with third parties without authorization, beyond the scope of the physician-patient relationship. These failures actually and proximately caused Plaintiffs' and Class Members' injuries.

247. As a direct, proximate, and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and Class Members have suffered or imminently will suffer injury and damages, including monetary damages, inappropriate advertisements and use of their Private Information for advertising purposes, and increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

248. Defendant's breach of its common-law duties to exercise reasonable care and negligence, directly and proximately caused Plaintiffs' and Class Members' actual, tangible, injury-in-fact and damages, including, without limitation: the unauthorized access of their Private Information by third parties; improper disclosure of their Private Information; receipt of targeted advertisements reflecting private medical information; lost benefit of their bargain; lost value of their Private Information and diminution in value; embarrassment, humiliation, frustration, and emotional distress; lost time and money incurred to mitigate and remediate the effects of use of their information, as to targeted advertisements that resulted from and were caused by Defendant's negligence; value to Plaintiffs and the Class Members of surrendering their choices to keep their Private Information private and allowing Defendant to track their data; increased risk of future harm resulting from future use and disclosure of Plaintiffs' and the Class Members' Private

Information; and other injuries and damages as set forth herein. These injuries are ongoing, imminent, immediate, and continuing.

249. Moreover, Plaintiffs' and the Class Members' foregoing personal injury and property damage was a sudden and dangerous occurrence because Plaintiffs and the Class entrusted their Private Information to Defendant within the scope the physician-patient relationship with the expectation that information would be kept confidential, and yet KSB suddenly, and without warning, disclosed that Private Information to others outside of the physician-patient relationship, without Plaintiffs' and the Class Members knowledge, consent, or authorization.

250. Defendant's negligence directly and proximately caused the unauthorized access and Disclosure of Plaintiffs' and Class Members' Private Information, PII and PHI, and as a result, Plaintiffs and Class Members have suffered and will continue to suffer damages as a result of Defendant's conduct. Plaintiffs and Class Members seek actual and compensatory damages, and all other relief they may be entitled to as a proximate result of Defendant's negligence.

251. Plaintiffs and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiffs and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Class)

252. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

253. Pursuant to the laws set forth herein, including the FTC Act, HIPAA, the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security

Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C and the other sections identified above, and Illinois law, including the Illinois Medical Patient Rights Act ("MPRA"), 410 Ill. Comp. Stat. 50/3(d), and the Illinois Personal Information Protection Act ("IPIPA"), 815 Ill. Comp. Stat. 530/5, /45, *et seq*., Defendant was required by law and industry standards to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiffs' and Class Members' Private Information.

254. Plaintiffs and Class Members are within the class of persons that these statutes and rules were designed to protect.

255. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' and Class Members' PII and PHI.

256. Defendant owed a duty to timely and adequately inform Plaintiffs and Class Members, in the event of their PII and PHI being improperly disclosed to unauthorized third parties.

257. It was not only reasonably foreseeable, but it was intended, that the failure to reasonably protect and secure Plaintiffs' and Class Members' PII and PHI in compliance with applicable laws would result in an unauthorized third-parties such as Facebook, and others gaining access to Plaintiffs' and Class Members' PII and PHI, and resulting in Defendant's liability under principles of negligence *per se*.

258. Defendant violated its duty under Section 5 of the FTC Act and/or HIPAA and/or under Illinois law by failing to use reasonable measures to protect Plaintiffs' and Class Members' PII and PHI and not complying with applicable industry standards as described in detail herein; as well as failing to disclose Defendant was gathering Private Information, including PHI and PII,

and sharing it with third parties without authorization, beyond the scope of the physician-patient relationship.

259. Plaintiffs' and Class Member's PII and PHI constitute personal property that was taken and misused as a proximate result of Defendant's negligence, resulting in harm, injury and damages to Plaintiffs and Class Members.

260. As a direct, proximate, and traceable result of Defendant's negligence *per se,* Plaintiffs and Class Members have suffered or imminently will suffer injury and damages, including monetary damages, inappropriate advertisements and use of their Private Information for advertising purposes, and increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

261. Defendant's breach of its duties and negligence *per se*, directly and proximately caused Plaintiffs' and Class Members' actual, tangible, injury-in-fact and damages, including, without limitation: the unauthorized access of their Private Information by third parties; improper disclosure of their Private Information; receipt of targeted advertisements reflecting private medical information; lost benefit of their bargain; lost value of their Private Information and diminution in value; embarrassment, humiliation, frustration, and emotional distress; lost use of their Private Information without compensation, and interference with their possession of their information; invasion of their privacy rights; lost time and money incurred to mitigate and remediate the effects of use of their information, as to targeted advertisements that resulted from and were caused by Defendant's negligence *per se*; value to Plaintiffs and the Class Members of surrendering their choices to keep their Private Information private and allowing Defendant to track their data; increased risk of future harm resulting from future use and disclosure of Plaintiffs' and the Class Members' Private Information; and other injuries and damages as set forth herein.

These injuries are ongoing, imminent, immediate, and continuing.

262. Moreover, Plaintiffs' and the Class Members' foregoing personal injury and property damage was a sudden and dangerous occurrence because Plaintiffs and the Class entrusted their Private Information to Defendant within the scope the physician-patient relationship with the expectation that information would be kept confidential, and yet KSB suddenly, and without warning, disclosed that Private Information to others outside of the physician-patient relationship, without Plaintiffs' and the Class Members knowledge, consent, or authorization.

263. Defendant's negligence *per se* directly and proximately caused the unauthorized access and Disclosure of Plaintiffs' and Class Members' Private Information, PII and PHI, and as a result, Plaintiffs and Class Members have suffered and will continue to suffer damages as a result of Defendant's conduct. Plaintiffs and Class Members seek actual and compensatory damages, and all other relief they may be entitled to as a proximate result of Defendant's negligence.

264. Plaintiffs and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's negligence *per se*, directed at injuring Plaintiffs and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

COUNT III
BREACH OF EXPRESS CONTRACT
(On Behalf of Plaintiffs and the Class)

265. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

266. Plaintiffs bring this claim for breach of express contract in the alternate to their negligence and negligence *per se* causes of action.

267. Plaintiffs and the proposed Class Members and Defendant entered into an express

agreement whereby Defendant agreed to provide medical care and treatment, and that in the course of providing said treatment, KSB would not disclose Plaintiffs' and the Class Private Information, including PHI, except as authorized.

268. In exchange, Plaintiffs and the proposed Class Members paid monies for treatment received and entrusted their Private Information to Defendant.

269. The express contact between Plaintiffs and the Class on the one hand, and Defendant on the other, was set forth in written Privacy Policies, including, but not limited to, KSB's Notice of Privacy Practices,[83] in which Defendant promised only to disclose Plaintiffs' and the Class Members' PHI for marketing purposes with said patients' written authorization.

270. Plaintiffs and Class Members fully performed their obligations under the express contract with Defendant. KSB did not. Plaintiffs and Class Members would not have provided their confidential Private Information to Defendant, and paid monies for treatment, in the absence of their express contracts with Defendant in which KSB promised to protect their Private Information, and Plaintiffs and the Class would have instead retained the opportunity to control their Private Information for uses other than receiving medical treatment from Defendant.

271. Defendant breached the express contract with Plaintiffs and the Class Members by disclosing their Private Information to third parties including Facebook, Google, and others, without written authorization, and in failing to apprise Plaintiffs and the Class Members of the unauthorized Disclosure, in violation of KSB's Privacy Policies.

272. As a direct and proximate result of Defendant's breach of contract, Plaintiffs and

[83] *See* KSB Patient Rights and Responsibilities, available at https://www.ksbhospital.com/your-rights-and-responsibilities/, and KSB Notice of Privacy Practices, available at https://www.ksbhospital.com/wordpress2017/wp-content/uploads/2023/07/npp_booklet_hc_provider-64a2ee1500642.pdf

the Class have suffered (and will continue to suffer) injury-in-fact and damages, including monetary damages; loss of privacy; unauthorized disclosure of Private Information; unauthorized access to Private Information by third parties; use of the Private Information for advertising purposes; embarrassment, humiliation, frustration, and emotional distress; decreased value of Private Information; lost benefit of the bargain; and increased risk of future harm resulting from further unauthorized use and disclosure of their information.

273. Further, non-economic damages are available to Plaintiffs and the Class Members because when Plaintiffs and the Class Members entered into the express contract, Defendant knew, or had reason to know, that its breach would cause mental suffering due to the disclosure and invasion of privacy itself, beyond mere pecuniary loss.

274. Specifically, Defendant knew, or had reason to know, that disclosing, without authorization, Private Information including PHI and PII to Facebook and other third parties, contrary to promises Defendant made, would cause mental suffering by virtue of the Disclosure, given that such information should reasonably be expected to be held in confidence and not disclosed to unauthorized third parties.

275. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiffs and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Class)

276. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

277. As a condition of receiving medical care from Defendant, Plaintiffs and the Class provided their Private Information and paid compensation for the treatment received.

278. In so doing, Plaintiffs and the Class entered into contracts with Defendant by which

Defendant agreed to safeguard and protect such information, in its Privacy Policies and elsewhere, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen. Implicit in the agreement between Defendant and its patients, Plaintiffs and the proposed Class Members, was the obligation that both parties would maintain the Private Information confidentially and securely.

279. KSB had an implied duty of good faith to ensure that the Private Information of Plaintiffs and Class Members in its possession was only used only as authorized, such as to provide medical treatment, billing, and other medical benefits from Defendant.

280. Defendant had an implied duty to protect the Private Information of Plaintiffs and Class Members from unauthorized disclosure or uses.

281. Additionally, Defendant implicitly promised to retain this Private Information only under conditions that kept such information secure and confidential.

282. Plaintiffs and Class Members fully performed their obligations under the implied contract with Defendant. KSB did not. Plaintiffs and Class Members would not have provided their confidential Private Information to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their Private Information for uses other than receiving medical treatment from Defendant.

283. Defendant breached the implied contracts with Plaintiffs and Class members by disclosing Plaintiffs' and Class Members' Private Information to unauthorized third parties, including Facebook, Google, and others.

284. Defendant's acts and omissions have materially affected the intended purpose of the implied contracts requiring Plaintiffs and Class Members to provide their Private Information in exchange for medical treatment and benefits.

285. As a direct and proximate result of Defendant's breach of contract, Plaintiffs and the Class have suffered (and will continue to suffer) injury-in-fact and damages, including monetary damages; loss of privacy; unauthorized disclosure of Private Information; unauthorized access to Private Information by third parties; use of the Private Information for advertising purposes; embarrassment, humiliation, frustration, and emotional distress; decreased value of Private Information; lost benefit of the bargain; and increased risk of future harm resulting from further unauthorized use and disclosure of their information.

286. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiffs and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT V
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

287. Plaintiffs re-allege and incorporate the preceding paragraphs as if fully set forth herein.

288. This claim is pleaded in the alternative to Plaintiffs' breach of implied contract claim.

289. Plaintiffs and Class Members conferred a monetary benefit upon Defendant in the form of valuable sensitive medical information—Private Information—that Defendant collected from Plaintiffs and Class Members under the guise of keeping this information private. Defendant collected, used, and disclosed this information for its own gain, for marketing purposes, and for sale or trade with third parties.

290. Plaintiffs and Class Members would not have used Defendant's services, or would have paid less for those services, if they had known that Defendant would collect, use, and disclose their Private Information to third parties.

291. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members.

292. As a result of Defendant's conduct, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy practices and procedures that Plaintiffs and Class Members paid for, and those purchases with unreasonable data privacy practices and procedures that they received.

293. The benefits that Defendant derived from Plaintiffs and Class Members rightly belong to Plaintiffs and Class Members themselves. Under unjust enrichment principles, it would be inequitable for Defendant to retain the profit and/or other benefits it derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Petition.

294. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds it received as a result of the conduct and the unauthorized Disclosure alleged herein.

COUNT VI
BAILMENT
(On Behalf of Plaintiffs and the Class)

295. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

296. Plaintiff, the Class, and Defendant contemplated a mutual benefit bailment when Plaintiffs and Class members transmitted their Private Information to Defendant solely for treatment and the payment thereof.

297. Plaintiffs' and the Class's Private Information was transmitted to Defendant in trust for a specific and sole purpose of receiving KSB 's medical treatment services, with an express contract that the trust was to be faithfully executed, and the Private Information was to be

accounted for when the special purpose was accomplished.

298. Defendant was duty bound under the law to exercise ordinary care and diligence in safeguarding Plaintiffs' and the Class's Private Information.

299. Plaintiffs' and the Class's Private Information was used for a different purpose than the Plaintiffs and the Class intended, for a longer time period and/or in a different manner or place than the parties intended. Instead of being used to facilitate their medical treatment, Plaintiffs' and the Class Members' Private Information was used by Defendant to benefit KSB and its marketing and advertising purposes.

300. Defendant's breach of the bailment was a legal cause of injury-in-fact and damage to Plaintiffs and the Class, including but not limited to, the unauthorized access of their Private Information by third parties, improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information, emotional distress and embarrassment and humiliation, and lost time and money incurred to mitigate and remediate the effects of use of their information that resulted from and were caused by Defendant's tortious conduct. These injuries are ongoing, imminent, immediate, and continuing.

301. As a direct and proximate result of Defendant's breach of the bailment, Plaintiffs and Class Members are entitled to and do demand actual, compensatory, and punitive damages, as well as injunctive relief, and all other relief allowed by law.

COUNT VII
VIOLATION OF THE ILLINOIS EAVESDROPPING STATUTE, 720 Ill. Comp. Stat. 5/14, *et seq*.
(On Behalf of Plaintiffs and the Class)

302. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

303. The Eavesdropping Article of the Illinois Criminal Code (the "Illinois Eavesdropping Statute" or "IES") states that it is a felony for any person to knowingly and

intentionally "use[] an eavesdropping devise, in a surreptitious manner, for the purpose of transmitting or recording all or part of any private conversation to which he or she is a party unless he or she does so with the consent of all other parties to the private conversation." 720 Ill. Comp. Stat. 5/14-2(a), -4.

304. The IES also states that it is a felony for any person to knowingly and intentionally "use[] or disclose[] any information which he or she knows or reasonably should know was obtained from a private conversation or private electronic communication in violation of this Article, unless he or she does so with the consent of all of the parties." *Id*.

305. For purposes of the IES, "eavesdropping device" means "any device capable of being used to hear or record oral conversation or intercept, or transcribe electronic communications whether such conversation or electronic communication is conducted in person, by telephone, or by any other means." 720 Ill. Comp. Stat. 5/14-1(a).

306. For purposes of the IES, "surreptitious" means "obtained or made by stealth or deception, or executed through secrecy or concealment." 720 Ill. Comp. Stat. 5/14-1(g).

307. For purposes of the IES, "private electronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire, radio, pager, computer, electromagnetic, photo electronic or photo optical system, when the sending or receiving party intends the electronic communication to be private under circumstances reasonably justifying that expectation. . . . Electronic communication does include any communication from a tracking device." 720 Ill. Comp. Stat. 5/14-1(e).

308. "A reasonable expectation shall include any expectation recognized by law, including, but not limited to, an expectation derived from a privilege, immunity, or right established by common law, Supreme Court rule, or the Illinois or United States Constitution." *Id*.

309. Defendant intentionally recorded and/or acquired Plaintiffs' and Class Members' private electronic communications, without the consent of Plaintiffs and Class Members, using the Pixel and similar tracking technologies on its Online Platforms.

310. Defendant intentionally recorded and/or acquired Plaintiffs' and Class Members' private electronic communications for the purpose of disclosing those communications to third parties, including Facebook and Google, without the knowledge, consent, or written authorization of Plaintiffs or Class Members.

311. Plaintiffs' and Class Members' communications with Defendant constitute private conversations, communications, and information.

312. Plaintiffs and Class Members had a reasonable expectation of privacy in their communications with Defendant via its Online Platforms.

313. Plaintiffs and Class Members communicated sensitive PHI and PII that they intended for only Defendant to receive and that they understood Defendant would keep private.

314. Plaintiffs and Class Members have a reasonable expectation that Defendant would not disclose PII, PHI, and confidential communications to third parties without Plaintiffs' or Class Members' authorization, consent, or knowledge.

315. Plaintiffs and Class Members had a reasonable expectation of privacy given Defendant's representations, Notice of Privacy Practices, and HIPAA. Moreover, Plaintiffs and Class Members have a general expectation that their communications regarding healthcare with their healthcare providers will be kept confidential.

316. Plaintiffs and Class Members were unaware that their Private Information was being surreptitiously recorded and transmitted to third parties as they communicated with Defendant through its Online Platforms.

317. Without Plaintiffs' or Class Members' knowledge, authorization, or consent, Defendant used the Pixel imbedded and concealed into the source code of its Online Platforms to secretly record and transmit Plaintiffs' and Class Members' private communications to hidden third parties, such as Facebook and Google, as described in the preceding paragraphs.

318. Under the IES, "[a]ny or all parties to any conversation or electronic communication upon which eavesdropping is practices contrary to this Article shall be entitled to the following remedies: (a) [t]o an injunction by the circuit court prohibiting further eavesdropping by the eavesdropper and by or on behalf of his principal, or either; (b) [t]o all actual damages against the eavesdropper or his principal or both; [t]o any punitive damages which may be awarded by the court or by a jury. . . ." 720 Ill. Comp. Stat. 5/14-6.

319. The eavesdropping devices used in this case include, but are not limited to:

a. Plaintiffs' and Class Members' personal computing devices;

b. Plaintiffs' and Class Members' web browsers;

c. Plaintiffs' and Class Members' browser-managed files;

d. Facebook's Pixel;

e. Internet cookies;

f. Other tracking technology including Google Analytics with Google Tag Manager ("GTM"), Innovid, and CallRail;

g. Defendant's computing servers;

h. Third-party source code utilized by Defendant; and

i. Computer servers of third-parties (including Facebook) to which Plaintiffs' and Class Members' communications were disclosed.

320. The eavesdropping devices outlined above are not excluded "tracking devices" as

that term is used in the IES, 720 ILCS 5/14-1(e), to the extent that they perform functions other than collection of geo-locational data.

321. Defendant is a "person" under the IES. 720 Ill. Comp. Stat. 5/2-15.

322. Defendant aided in the interception of communications between Plaintiffs and Class Members and Defendant that were redirected to and recorded by third parties without Plaintiffs' or Class Members' consent.

323. Under the IES, Plaintiffs and the Class Members are entitled to injunctive relief prohibiting further eavesdropping by Defendant, actual damages, and punitive damages.

324. Defendant's violation of the IES caused Plaintiffs and Class Members the following damages:

a. Sensitive and confidential information that Plaintiffs and Class Members
b. intended to remain private is no longer private;
c. Defendant eroded the essential confidential nature of the physician-patient relationship;
d. Defendant took something of value from Plaintiffs and Class Members and derived benefit therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without sharing the benefit of such value;
e. Plaintiffs and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality; and
f. Defendant's actions diminished the value of Plaintiffs' and Class Members' Private Information.

325. Plaintiffs and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

COUNT VIII
VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA")
18 U.S.C. §§ 2511(1), *et seq.*
(On Behalf of Plaintiffs and the Class)

326. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

327. The ECPA protects both sending and receipt of communications. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

328. The transmissions of Plaintiffs' and Class Members' Private Information to Defendant's Website qualifies as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

329. **Electronic Communications**. The transmission of Private Information between Plaintiffs and Class Members and Defendant's Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo optical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

330. **Content**. The ECPA defines content, when used with respect to electronic communications, to "include [] any information concerning the substance, purport, or meaning of that communication." *See* 18 U.S.C. § 2510(8).

331. **Interception**. The ECPA defines the interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents…include any information concerning the substance, purport, or meaning of that communication." See 18 U.S.C. § 2510(4), (8).

332. **Electronic, Mechanical or Other Device**. The ECPA defines "electronic,

mechanical, or other device" as "any device…which can be used to intercept a[n]…electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. Plaintiffs' and Class Members' browsers;

b. Plaintiffs' and Class Members' computing devices;

c. Defendant's web-servers; and

d. Defendant's Website.

333. The tracking technology deployed by Defendant effectuated the sending and acquisition of patient communications.

334. By utilizing and embedding the tracking technology on its Website, Defendant intentionally intercepted, endeavored to intercept and procured another person to intercept the electronic communications of Plaintiffs and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

335. Specifically, Defendant intercepted Plaintiffs' and Class Members' electronic communications via the tracking technology including the Pixel, which tracked, stored ,and unlawfully disclosed Plaintiffs' and Class Members' Private Information to Facebook, Google, DoubleClick, the Trade Desk, and Frequence.

336. Defendant's intercepted communications include, but are not limited to, communications to/from Plaintiffs and Class Members regarding Private Information, and medical treatment.

337. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiffs and Class Members to third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication

in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

338. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiffs and Class Members, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

339. **Unauthorized Purpose.** Defendant intentionally intercepted the contents of Plaintiffs' and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State – namely, invasion of privacy, among others.

340. Defendant intentionally used the wire or electronic communications to increase its profit margins and save on marketing costs.

341. Defendant specifically used the Pixel to track and to utilize Plaintiffs' and Class Members' Private Information for financial gain.

342. Defendant was not acting under color of law to intercept Plaintiffs' and Class Members' wire or electronic communication.

343. Plaintiffs and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiffs' and Class Members' privacy via the tracking technology.

344. In sending and in acquiring the content of Plaintiffs' and Class Members' communications relating to the browsing of its Website, Defendant's purpose was tortious, criminal and designed to violate federal and state legal provisions, including as described above the following: (i) a knowing intrusion into a private, place, conversation or matter that would be highly offensive to a reasonable person; and (ii) violation of HIPAA, the FTC Act, invading

Plaintiffs and Class Members' privacy, and in breach of its fiduciary duty of confidentiality.

COUNT IX
VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA")
18 U.S.C. § 2511(3)(a)
UNAUTHORIZED DIVULGENCE BY ELECTRONIC COMMUNICATIONS SERVICE
(On Behalf of Plaintiffs and the Class)

345. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

346. The ECPA statute provides that "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." 18 U.S.C. § 2511(3)(a).

347. **Electronic Communication Service**. An "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). Defendant's Website is an electronic communication service which provides to users thereof, patients of Defendant, the ability to send or receive electronic communications; in the absence of Defendant's Website, internet users could not send or receive communications regarding Plaintiffs' and Class Members' Private Information.

348. **Intentional Divulgence**. Defendant intentionally designed the tracking technology and was or should have been aware that, if so configured, it could divulge Plaintiffs' and Class Members' Private Information. Upon information and belief, Defendant's divulgence of the contents of Plaintiffs' and Class Members' communications was contemporaneous with their exchange with Defendant's Website, to which they directed their communications.

349. Defendant divulged the contents of Plaintiffs' and Class Members' electronic communications without authorization and/or consent.

350. **Exceptions do not apply**. In addition to the exception for communications directly to an electronic communications service ("ECS")[84] or an agent of an ECS, the ECPA states that "[a] person or entity providing electronic communication service to the public may divulge the contents of any such communication."

a. "as otherwise authorized in section 2511(2)(a) or 2517 of this title;

b. "with the lawful consent of the originator or any addressee or intended recipient of such communication;" c. "to a person employed or authorized, or whose facilities are used, to forward such communication to its destination;" or d. "which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency." U.S.C. § 2511(3)(b).

351. Section 2511(2)(a)(i) provides: It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

352. Defendant's divulgence of the contents of Plaintiffs' and Class Members' communications to Facebook was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (i) a necessary incident to the rendition of Defendant's service nor (ii) necessary to the protection

[84] An ECS is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

of the rights or property of Defendant.

353. Section 2517 of the ECPA relates to investigations by government officials and has no relevance here.

354. Defendant's divulgence of the contents of Plaintiffs' and the Class Members' patient user communications on its Website through the tracking technology was not done "with the lawful consent of the originator or any addresses or intended recipient of such communication[s]." As alleged above: (i) Plaintiffs and Class Members did not authorize Defendant to divulge the contents of their communications and (ii) Defendant did not procure the "lawful consent" from the websites or apps with which Plaintiffs and Class Members were exchanging information.

355. Moreover, Defendant divulged the contents of Plaintiffs' and Class Members' communications through the Pixel code to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

356. The contents of Plaintiffs' and Class Members' communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their communications to a law enforcement agency.

357. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages, preliminary and other equitable or declaratory relief as may be appropriate, punitive damages in an amount to be determined by a jury and a reasonable attorney's fee and other litigation costs reasonably incurred.

COUNT X
VIOLATION OF TITLE II OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT ("STORED COMMUNICATIONS ACT")
18 U.S.C. § 2702, *et seq.*
(On Behalf of Plaintiffs and the Class)

358. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

359. The ECPA further provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

360. **Electronic Communication Service**. ECPA defines "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). Defendant intentionally procures and embeds various Plaintiffs' and Class Members' patient Private Information through the tracking technology used on Defendant's Website, which qualifies as an Electronic Communication Service.

361. **Electronic Storage**. ECPA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

362. Defendant stores the content of Plaintiffs' and Class Members' communications on Defendant's Website and files associated with it.

363. When Plaintiffs or Class Members make a Website communication, the content of that communication is immediately placed into storage.

364. Defendant knowingly divulges the contents of Plaintiffs' and Class Members' communications through the tracking technology.

365. **Exceptions Do Not Apply**. Section 2702(b) of the Stored Communication Act provides that an electronic communication service provider "may divulge the contents of a communication—" a. "to an addressee or intended recipient of such communication or an agent of

such addressee or intended recipient." b. "as otherwise authorized in Section 2517, 2511(2)(a), or 2703 of this title;" c. "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;" d. "to a person employed or authorized or whose facilities are used to forward such communication to its destination;" e. "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;" f. "to the National Center for Missing and Exploited Children, in connection with a reported submission thereto under section 2258A." g. "to a law enforcement agency, if the contents (i) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime;" h. "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency"; or "to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies Section 2523."

366. Defendant did not divulge the contents of Plaintiffs' and Class Members' communications to "addressees," "intended recipients," or "agents" of any such addressees or intended recipients of Plaintiffs and Class Members.

367. Section 2517 and 2703 of the ECPA relate to investigations by government officials and have no relevance here.

368. Section 2511(2)(a)(i) provides: It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his

employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

369. Defendant's divulgence of the contents of Plaintiffs' and Class Members' communications on its Website to Facebook or other third parties was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (i) a necessary incident to the rendition of the Defendant's services nor (ii) necessary to the protection of the rights or property of Defendant.

370. Section 2517 of the ECPA relates to investigations by government officials and has no relevance here.

371. Defendant's divulgence of the contents of Plaintiffs' and Class Members' patient user communications on its Website was not done "with the lawful consent of the originator or any addresses or intended recipient of such communication[s]." As alleged above: (i) Plaintiffs and Class Members did not authorize Defendant to divulge the contents of their communications and (ii) Defendant did not procure the "lawful consent" from the websites or apps with which Plaintiffs and Class Members were exchanging information.

372. Moreover, Defendant divulged the contents of Plaintiffs' and Class Members' communications through the tracking technology to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

373. The contents of Plaintiffs' and Class Members' communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their communications to a law enforcement agency.

374. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may

assess statutory damages, preliminary and other equitable or declaratory relief as may be appropriate, punitive damages in an amount to be determined by a jury and a reasonable attorney's fee and other litigation costs reasonably incurred.

COUNT XI
VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT ("CFAA")
18 U.S.C. § 1030, *et seq.*
(On Behalf of Plaintiffs and the Class)

375. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

376. Plaintiffs' and the Class Members' computers and mobile devices are, and at all relevant times have been, used for interstate communication and commerce, and are therefore "protected computers" under 18 U.S.C. § 1030(e)(2)(B).

377. Defendant exceeded, and continues to exceed, authorized access to Plaintiffs' and the Class Members' protected computers and obtained information thereby, in violation of 18 U.S.C. § 1030(a)(2), (a)(2)(C).

378. Defendant's conduct caused "loss to 1 or more persons during any 1-year period… aggregating at least $5,000 in value" under 18 U.S.C. § 1030(c)(4)(A)(i)(I), *inter alia*, because of the secret transmission of Plaintiffs' and the Class Members' Private Information as set forth in detail herein, which were never intended for public consumption.

379. Defendant's conduct also constitutes "a threat to public health or safety" under 18 U.S.C. § 1030(c)(4)(A)(i)(IV), due to the private and personally identifiable data and content of Plaintiffs and the Class Members' Private Information and communication being made available to Defendant, Facebook, Google, and/or other third parties without adequate legal privacy protections.

380. Accordingly, Plaintiffs and the Class Members are entitled to "maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable

relief." 18 U.S.C. § 1030(g).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Chloe Noftz, Tonya Black and Kenneth Weinstock, on behalf of themselves and on behalf of all others similarly situated, prays for judgment as follows:

a. for an Order certifying this action as a Class action and appointing Plaintiffs as Class Representative and Plaintiffs' counsel as Class Counsel;

b. for an award of actual damages, compensatory damages, consequential damages, and punitive damages, in an amount to be determined, as allowable by law;

c. for equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs and Class Members;

d. for equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity the type of Private Information compromised and unlawfully disclosed to third parties;

e. for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

f. for an award of attorneys' fees under the common fund doctrine, and any other applicable law;

g. costs and any other expenses, including expert witness fees incurred by Plaintiffs in connection with this action;

h. pre- and post-judgment interest on any amounts awarded; and

i. such other and further relief as this court may deem just and proper.

JURY DEMAND

Plaintiffs, on behalf of themselves and all others similarly situated, hereby demand a trial by jury on all issues so triable.

Respectfully submitted,

/s/ Samuel J. Strauss

Samuel J. Strauss (ARDC No. 6340331)
Raina C. Borrelli (ARDC No. 6340619)
Strauss Borelli PLLC
One Magnificent Mile
980 North Michigan Avenue, Suite 1610
Chicago, Illinois 60611
(872) 263-1100
sam@straussborrelli.com
raina@straussborrelli.com

Lynn A. Toops (*Pro Hac Vice* forthcoming)
Amina A. Thomas (*Pro Hac Vice* forthcoming)
Mallory K. Schiller (*Pro Hac Vice* forthcoming)
Cohen & Malad, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com
athomas@cohenandmalad.com
mschiller@cohenandmalad.com

J. Gerard Stranch, IV (*Pro Hac Vice* forthcoming)
Andrew E. Mize (*Pro Hac Vice* forthcoming)
Emily E. Schiller (*Pro Hac Vice* forthcoming)
Stranch, Jennings & Garvey, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)
gstranch@stranchlaw.com
amize@stranchlaw.com
eschiller@stranchlaw.com

Counsel for Plaintiffs and the Proposed Class